Plan d'action du Conseil canadien
de la magistrature en matière de

Sécurité des renseignements judiciaires

Deuxième édition, 2006

Révisé le 5 septembre 2006

Produit par le Sous-comité de la sécurité informatique du Comité consultatif sur la technologie

Table des matières

Sommaire

1. Le présent Plan d'action vise plusieurs objectifs. Le principal d'entre eux consiste à fournir des lignes de conduite afin d'améliorer la sécurité, l'accessibilité et l'intégrité des systèmes informatiques contenant des renseignements judiciaires. Il vise également à définir clairement les rôles et responsabilités respectifs des juges et des administrateurs en ce qui concerne la sécurité des technologies de l'information et à améliorer les relations entre les deux groupes. Enfin, le Plan d'action est conçu de manière à fournir aux juges de l'ensemble du Canada un modèle pour l'élaboration de politiques efficaces relatives à la sécurité des technologies de l'information qui tiennent compte des besoins de la magistrature.

2. Le Conseil canadien de la magistrature (le Conseil) est préoccupé par le fait que le niveau de sécurité des renseignements judiciaires dans l'ensemble du Canada est inégal et différent d'une juridiction à l'autre. La sécurité des renseignements judiciaires devrait être uniformisée le plus possible parmi l'ensemble des cours. Des pratiques exemplaires devraient être arrêtées et mises en oeuvre dans tous les cas.

3. Le Conseil est également préoccupé par le fait que, plus souvent qu'autrement, les juges ne participent pas à la formulation des politiques. Le Conseil veut s'assurer que les juges jouent un plus grand rôle dans l'élaboration des politiques et que toutes les mesures de sécurité prises par les cours soient compatibles avec les principes fondamentaux de l'indépendance judiciaire[1].

4. Le Plan d'action s'applique à tout système informatique dans lequel des renseignements judiciaires (tels qu'ils sont définis dans le Plan d'action) sont créés, enregistrés ou transmis. Cela comprend les ordinateurs domestiques, les appareils portatifs et les périphériques, s'ils contiennent des renseignements judiciaires.

---

[1] En septembre 2002, le Comité spécial sur les orientations futures du Conseil a publié un rapport, intitulé « La voie à suivre », qui recommande que le Conseil assume un rôle de leadership à l'égard de l'utilisation des technologies de l'information dans les cours supérieures. Voir le site Web du Conseil à l'adresse www.cjc-ccm.gc.ca .

5. Le Conseil reconnaît que certaines cours du Canada ont adopté des politiques et programmes de gestion complexes en matière de sécurité informatique. Le Plan d'action vise à améliorer ces politiques et programmes et à les remplacer uniquement s'ils vont à l'encontre de ceux qui sont proposés dans le présent document ou s'ils sont moins stricts que ceux-ci. Le Plan d'action n'a pas pour but de dégager les cours de leurs responsabilités individuelles en ce qui a trait à l'évaluation des menaces et des risques dans leur environnement spécifique.

6. Si un seul utilisateur – qu'il s'agisse ou non d'un juge – omet d'observer une norme de sécurité appropriée, cela risque de compromettre l'ensemble du réseau ainsi que la sécurité des renseignements judiciaires de tous les juges et des autres utilisateurs du réseau. C'est pourquoi le Conseil encourage tous les juges et les autres utilisateurs du système judiciaire à adopter les politiques et pratiques énoncées dans le présent document, non seulement dans l'intérêt de l'appareil judiciaire, mais également pour les tierces parties dont les renseignements nécessitent une protection spéciale en vertu de la loi.

7. Le Plan d'action énonce seize politiques de haut niveau que les cours sont encouragées à mettre en œuvre. Chaque énoncé de politique est suivi de commentaires et d'une série d'exemples de lignes directrices visant à en illustrer l'application. Le document ne se veut pas un manuel technique, bien qu'il comporte plusieurs renvois à des publications dont l'approche est davantage axée sur les aspects techniques. Le présent document a plutôt pour but d'informer les juges et de fournir des paramètres de base à partir desquels chaque cour pourra adopter des mesures de sécurité efficaces.

8. Le Plan d'action est divisé en trois sections qui correspondent aux trois types de mesures de protection en matière de sécurité. Le premier groupe de politiques concerne la gestion de la sécurité des technologies de l'information.

Politique 1 : Chaque juridiction doit veiller à ce qu'un agent de la sécurité informatique du système judiciaire responsable envers la magistrature soit nommé et chargé de surveiller la gestion des mesures de sécurité relatives aux technologies de l'information des cours.

Politique 2 : La planification relative à la sécurité des technologies de l'information et l'élaboration de politiques visant à assurer la protection des renseignements judiciaires sont des fonctions judiciaires. La magistrature doit prendre la responsabilité de l'élaboration des politiques qui touchent les utilisateurs judiciaires ou la façon dont ils exercent leurs fonctions. Toutes les politiques des cours en matière de sécurité doivent être interprétées et appliquées conformément aux Lignes de conduite sur la surveillance *informatique du Conseil.*

Politique 3 : Les cours doivent offrir à tous les utilisateurs une formation continue en matière de sensibilisation à la sécurité informatique ainsi que de la documentation connexe, et tous les membres du personnel informatique qui utilisent des renseignements judiciaires dans le cadre de leur travail doivent obligatoirement suivre une formation approfondie en matière de sécurité informatique.

Politique 4 : Chaque cour doit planifier et effectuer régulièrement une évaluation des menaces et des risques (EMR). Le niveau de détail, l'ampleur et la fréquence de l'EMR varieront selon le niveau de risque.

9. La principale recommandation est que chaque juridiction nomme un agent de la sécurité informatique du système judiciaire, dont les qualifications et les fonctions sont énoncées dans le Plan d'action. L'agent de la sécurité informatique du système judiciaire devrait être un spécialiste en technologies de l'information qui possède de l'expérience technique et une bonne connaissance des protocoles de sécurité qui conviennent à la taille et à la complexité du système informatique de la cour. Cette personne doit être nommée à un poste de niveau de gestion, elle doit être capable de représenter la magistrature en ce qui a trait à la sécurité informatique et elle doit relever du juge en chef.

10. L'agent de la sécurité informatique du système judiciaire serait responsable de fournir à la magistrature des avis impartiaux sur toutes les questions concernant la sécurité de l'informatique et d'effectuer des vérifications périodiques de la sécurité des systèmes informatiques qui contiennent des renseignements judiciaires. De plus, l'agent de la sécurité informatique du système judiciaire aurait la responsabilité générale des questions de sécurité informatique qui relèvent principalement de la magistrature, notamment l'élaboration des politiques, l'évaluation des risques et l'assurance de la conformité aux politiques et normes telles que le Plan d'action et la norme ISO 17799.

11. La deuxième section concerne les mesures de protection opérationnelles, y compris la sauvegarde et la sécurité matérielle, et elle propose un système de classification des renseignements judiciaires.

Politique 5 : Les cours doivent protéger les renseignements judiciaires en cas de catastrophe ou de défaillance du système et fournir un degré élevé d'assurance que le service interrompu par suite d'un tel événement sera rétabli dans les meilleurs délais. Les utilisateurs judiciaires doivent avoir accès au stockage réseau et le contenu de celui-ci doit être sauvegardé au moins une fois par jour. Des dispositions efficaces doivent être prises en vue de faciliter la sauvegarde des renseignements judiciaires créés ou reçus et stockés localement, par exemple sur des ordinateurs portatifs pendant les déplacements.

Politique 6 : Tous les éléments critiques de l'équipement de réseautique devraient se trouver dans un environnement à accès contrôlé et limité au personnel responsable de leur administration et de leur maintenance. Le local doit être muni de dispositifs de contrôle de l'environnement satisfaisants. Si les utilisateurs judiciaires se servent d'ordinateurs portatifs, des mécanismes comme des dispositifs de verrouillage et des avertisseurs devraient être fournis et utilisés de façon à réduire les risques de vol. Le chiffrement du disque est fortement recommandé pour tous les ordinateurs portatifs. Des mesures comme la tenue de registres de contrôle d'accès et la surveillance par caméra vidéo de l'équipement de réseautique devraient être mises en oeuvre. Les cours doivent veiller à ce qu'aucun renseignement judiciaire ne puisse être récupéré lorsqu'elles se débarrassent d'un dispositif informatique ou d'un support de données (y compris les rubans magnétiques servant aux sauvegardes).

Politique 7 : Les cours devraient adopter un système de classification permettant l'identification des renseignements judiciaires sensibles afin de leur assurer une protection spéciale. Les renseignements classifiés doivent être divulgués uniquement aux personnes qui ont besoin de les connaître.

12. Selon le système de classification, les renseignements sensibles devraient être identifiés par la mention « Renseignements réservés aux utilisateurs judiciaires » ou « Renseignements protégés ». Les renseignements ainsi classifiés devraient faire l'objet de procédures spéciales visant à en protéger la confidentialité.

13. La dernière grande section énonce les politiques concernant les mesures de protection techniques comme les systèmes de contrôle relatifs à l'accès local et à l'accès à distance, les techniques de chiffrement, les pare-feux et les systèmes de détection d'intrusion et de virus.

Politique 8 : Les cours doivent mettre en oeuvre des mesures de contrôle d'accès strictes afin que seuls les utilisateurs autorisés aient accès aux systèmes judiciaires et que leur niveau d'accès corresponde à l'autorisation d'accès qu'ils ont obtenue ainsi qu'au système de classification des renseignements de la cour concernée. Il appartient aux juges de déterminer les droits d'accès aux renseignements judiciaires classifiés.

Politique 9 : Des mesures spéciales doivent être prises pour assurer la sécurité et la confidentialité de toutes les connexions à distance et de la réseautique sans fil.

Politique 10 : La configuration des systèmes de contrôle d'accès des cours doit être conforme au principe de l'indépendance judiciaire. Les utilisateurs judiciaires devraient disposer d'un accès exclusif à leurs propres ressources réseau, à moins qu'il ne puisse être démontré que l'architecture, la configuration, les mécanismes de contrôle d'accès, le soutien opérationnel et les systèmes de classification des renseignements du réseau concerné soient suffisants pour assurer une confiance absolue dans la séparation des renseignements judiciaires et non judiciaires et pour assurer la conformité au Plan d'action et aux Lignes de conduite sur la surveillance informatique du Conseil.

Politique 11 : Les cours doivent mettre à la disposition des utilisateurs judiciaires une technologie de chiffrement à jour pour le stockage et la transmission des renseignements judiciaires classifiés sur les réseaux, les ordinateurs de bureau et les ordinateurs portatifs.

Politique 12 : Tous les réseaux des cours où se trouvent des renseignements judiciaires doivent être protégés des réseaux extérieurs, y compris Internet, au moyen d'une technologie de pare-feu appropriée qui est administrée de manière efficace. Toutes les connexions depuis un réseau de la cour à des réseaux extérieurs doivent passer par des pare-feux approuvés.

Politique 13 : Les cours doivent établir une procédure d'ouverture de session sur tous les serveurs et dispositifs du réseau afin de détecter les tentatives d'accès non autorisé et les séquences d'opérations suspectes. Toute activité de ce type de la part des utilisateurs judiciaires est assujettie en tout temps aux Lignes de conduite sur la surveillance informatique et doit être portée à l'attention de l'agent de la sécurité informatique du système judiciaire. Dans les cas où l'EMR le recommande, les cours devraient installer des systèmes de détection d'intrusion en versions réseau et intégrée assurant un signalement automatique des intrusions en temps réel.

Politique 14 : Tous les systèmes des cours doivent employer des logiciels conformes aux normes de l'industrie pour assurer la détection en temps réel des codes malveillants, du pourriel et des menaces connexes et pour assurer une protection contre ceux-ci.

Politique 15 : Dans toute la mesure du possible, de tels systèmes de protection doivent être installés sur les pare-feux, les serveurs, les postes de travail locaux, les ordinateurs portatifs, les appareils portatifs et les ordinateurs domestiques qui renferment des renseignements judiciaires ou qui servent à accéder à de tels renseignements.

Politique 16 : Tous les utilisateurs doivent recevoir une formation sur les pratiques exemplaires à suivre pour réduire les risques de codes malveillants, de pourriel et de menaces connexes.

14. Les commentaires sur l'indépendance judiciaire, qui suivent l'énoncé de politique 10, sont l'un des principaux aspects de cette section. La politique suppose que seuls les utilisateurs judiciaires ont accès aux systèmes contenant des renseignements judiciaires, à moins que des mesures opérationnelles et techniques efficaces ne soient prises pour assurer une séparation réelle.

15. Les Lignes de conduite sur la surveillance informatique, qui présentent le point de vue du Conseil sur la façon dont la surveillance des activités informatiques judiciaires devrait être restreinte, sont jointes à l'annexe 2 du Plan d'action. Le Modèle de règles d'utilisation acceptable des ordinateurs pour le personnel judiciaire, adopté par le Conseil, est joint à l'annexe 6.

Introduction

16. Le présent Plan d'action vise plusieurs objectifs. Le principal d'entre eux consiste à fournir des lignes de conduite afin d'améliorer la sécurité, l'accessibilité et l'intégrité des systèmes informatiques contenant des renseignements judiciaires. Il vise également à définir clairement les rôles et responsabilités respectifs des juges et des administrateurs en ce qui concerne la sécurité des technologies de l'information et à améliorer les relations entre les deux groupes. Enfin, le Plan d'action est conçu de manière à fournir aux juges de l'ensemble du Canada un modèle pour l'élaboration de politiques efficaces relatives à la sécurité des technologies de l'information qui tiennent compte des besoins de la magistrature.

17. Le Conseil canadien de la magistrature (le Conseil) est préoccupé par le fait que le niveau de sécurité des renseignements judiciaires dans l'ensemble du Canada est inégal et différent d'une juridiction à l'autre. La sécurité des renseignements judiciaires devrait être uniformisée le plus possible parmi l'ensemble des cours. Des pratiques exemplaires devraient être arrêtées et mises en oeuvre dans tous les cas.

18. Le Conseil est également préoccupé par le fait que, plus souvent qu'autrement, les juges ne participent pas à la formulation des politiques. Le Conseil veut s'assurer que les juges jouent un plus grand rôle dans l'élaboration des politiques et que toutes les mesures de sécurité prises par les cours soient compatibles avec les principes fondamentaux de l'indépendance judiciaire.

19. En ce qui concerne les juges, la sécurité des renseignements présente des défis d'ordre pratique en raison de la situation constitutionnelle unique du Canada. Par exemple, dans la plupart des cours, des administrateurs qui ne relèvent pas de l'autorité judiciaire fournissent tous les services informatiques aux juges. Non seulement la ligne qui sépare les juges et ces administrateurs est-elle mal définie, mais il est rare qu'un lien hiérarchique existe entre les deux groupes. C'est ce qui explique qu'il est parfois difficile pour les administrateurs d'obtenir la collaboration des juges au plan de l'application d'une politique informatique, tout comme il peut être difficile pour les juges de diriger les travaux du personnel de soutien technique.

20. Le Conseil suggère que les administrateurs de l'informatique, le personnel de soutien et le personnel des services de dépannage qui travaillent avec les utilisateurs judiciaires soient mis au courant de la nature du rôle et de la fonction judiciaire dans le cadre de l'administration de la justice. Toutes ces personnes doivent faire la distinction entre les utilisateurs judiciaires et les autres utilisateurs afin de préserver l'indépendance de la magistrature.

21. Le Conseil canadien de la magistrature se fonde sur plusieurs recommandations qui ont été formulées en novembre 2001[2] et qui reposent sur les principes fondamentaux suivants :

    - Les juges et les administrateurs des cours doivent faire de la sécurité des technologies de l'information (sécurité informatique) une priorité au sein de leurs cours.

    - La sécurité informatique n'est pas seulement une préoccupation d'ordre technique; elle met aussi en cause les méthodes de planification, de gestion et d'exploitation ainsi que les pratiques des utilisateurs finals.

    - Toutes les mesures que prennent les cours en matière sécurité informatique doivent préserver l'indépendance judiciaire ainsi que les autres aspects uniques des rapports entre les utilisateurs judiciaires et le personnel chargé de l'administration des systèmes informatiques au sein des cours, que la gestion relève du gouvernement, d'un organisme offrant des services judiciaires ou même du secteur privé.

    - La responsabilité relative aux politiques de sécurité informatique *en ce qui concerne les renseignements judiciaires* est une fonction judiciaire et relève donc de la magistrature.

    - La gestion, l'exploitation et les mesures techniques visant à protéger les renseignements judiciaires conformément à la politique judiciaire sont des fonctions administratives qui relèvent, dans le cas de la plupart des cours, du gouvernement provincial[3].

22. Le Plan d'action constitue une partie de l'approche du Conseil à l'égard de la sécurité des renseignements judiciaires.[4] Les autres éléments de cette approche comprennent :

    - les Lignes de conduite sur la surveillance informatique (2002) (annexe 2);

    - le Protocole type pour les comités de technologie des tribunaux (2004) (annexe 3);

    - « La protection en dix points des renseignements judiciaires informatisés » (deuxième édition, 2006) (annexe 4);

---

2 Voir l'annexe 1. Le rapport de 2001 est confidentiel, car il traite des vulnérabilités des systèmes judiciaires.

3 Cette question ne se pose pas dans le cas des cours fédérales comme la Cour suprême du Canada.

4 Pour obtenir plus de renseignements sur les initiatives du Conseil en matière de sécurité des renseignements, veuillez consulter le site Web du Conseil à l'adresse www.cjc-ccm.gc.ca .

- les mesures d'élimination des métadonnées[5];
- la collaboration avec le Bureau du commissaire à la magistrature fédérale (CMF) et l'Institut national de la magistrature (INM) en ce qui a trait à la formation en matière de sécurité informatique;
- le Modèle de règles d'utilisation acceptable des ordinateurs pour le personnel judiciaire (2003) (annexe 6).

Portée et application

23. Même si le mandat légal du Conseil vise seulement les juges nommés par le gouvernement fédéral, il arrive souvent que ces juges partagent des ressources informatiques avec leurs collègues nommés par les gouvernements provinciaux. Cette seule raison suffit à encourager la collaboration à l'égard de l'élaboration des politiques en matière de sécurité. De plus, bon nombre de juges utilisent les ressources de Judicom, le réseau de communication judiciaire[6].

24. Le Plan d'action s'applique à tout système informatique dans lequel des renseignements judiciaires sont créés, enregistrés ou transmis. Cela comprend les ordinateurs domestiques, les appareils portatifs et les périphériques, s'ils contiennent des renseignements judiciaires.

25. Les « renseignements judiciaires » sont des renseignements qui sont recueillis, produits ou utilisés à des fins judiciaires, sauf :

    a) les politiques et procédures administratives des services judiciaires et les renseignements recueillis ou produits expressément pour la gestion de ces politiques et procédures administratives;
    b) les listes chronologiques des instances judiciaires;
    c) les pièces, les affidavits et les autres preuves documentaires qui sont déposés à la cour;
    d) les documents, les décisions, les certificats, les ordonnances, les jugements et les motifs de jugement qui sont publiés.

---

5 Voir, par exemple, l'article intitulé « La préparation des documents pour distribution électronique », rédigé par Frédéric Pelletier et Daniel Poulin, à l'adresse http://www.lexum.umontreal.ca/ccc-ccr/guide/docs/distribution_fr.html , qui accompagne le document intitulé « Le Guide canadien pour la préparation uniforme des jugements », adopté par le Conseil canadien de la magistrature en septembre 2002.

6 Le réseau Judicom a été créé par le Bureau du commissaire à la magistrature fédérale.

26. Les renseignements judiciaires sont créés par les juges, y compris les fonctionnaires judiciaires comme les conseillers-maîtres, les greffiers et les protonotaires, ainsi que par le « personnel judiciaire », notamment les employés ou les entrepreneurs qui travaillent pour le compte des juges et dont le travail comprend le traitement de renseignements judiciaires, comme les attachés de direction, les stagiaires et les étudiants en droit, ainsi que les adjoints et les secrétaires judiciaires. Ensemble, les juges et le personnel judiciaire sont appelés les « utilisateurs judiciaires ».

27. La sécurité des systèmes informatiques est un domaine complexe et le Plan d'action ne peut en couvrir tous les aspects. Le lecteur est prié de consulter les normes, ouvrages et documents mentionnés dans les références indiquées ci-dessous. De plus, le Conseil s'intéresse principalement au rôle de la magistrature dans l'élaboration des normes et politiques et non pas aux détails de la gestion d'un service informatique. À cet égard, le Plan d'action ne couvre pas chacun des aspects de l'administration de la sécurité. Par exemple, il ne traite pas de la conformité aux lois sur le droit d'auteur ou sur les permis d'utilisation de logiciel. (Voir la norme ISO 17799, section 15.[7]) Il ne traite pas non plus de la sécurité relative au soutien et à l'exploitation des systèmes informatiques, de la sécurité des renseignements qui ne sont pas sous forme numérique, de la sécurité des communications par téléphone ou par télécopieur, ni de la sécurité physique des palais de justice. Pour plus d'information sur la sécurité de l'exploitation des systèmes informatiques, il y a lieu de consulter le chapitre 14 du Manuel du CST[8]. La norme ISO 17799 traite de la sécurité des communications par téléphone et par télécopieur.

28. Le Conseil reconnaît que certaines cours du Canada ont adopté des politiques et programmes de gestion complexes en matière de sécurité informatique. Le Plan d'action vise à améliorer ces politiques et programmes et à les remplacer *uniquement s'ils vont à l'encontre de ceux qui sont proposés dans le présent document ou s'ils sont moins stricts que ceux-ci*. Dans cette mesure, le Plan d'action est conçu en grande partie pour être utilisé conjointement avec le Manuel du CST (Canada), la norme ISO 17799 (britannique/internationale) et le *NIST Handbook*[9] (États-Unis).

---

7 Tous les renvois concernent la norme ISO/IEC 17799:2005.

8 Centre de la sécurité des télécommunications, Manuel canadien de la sécurité des technologies de l'information, mars 1998 (« Manuel du CST »). Des exemplaires du manuel sont offerts gratuitement en français à http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-f.html et en anglais à http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-e.html .

9 National Institute of Standards and Technology, US Department of Commerce, "An Introduction to Computer Security: the NIST Handbook." Offert gratuitement à http://csrc.nist.gov/publications/nistpubs/800-12/ .

Conformité

29. Les politiques et normes de sécurité informatique se veulent impératives. Le respect universel des exigences en matière de sécurité protège tous les utilisateurs d’une organisation. Cependant, les juges sont différents des autres utilisateurs en ce qui a trait à au moins un aspect vital : ils ne sont pas assujettis à la surveillance ni aux procédures disciplinaires de l’organisme qui assure leurs besoins informatiques.

30. L’idée même que certaines politiques ou procédures soient impératives préoccupe de nombreux juges. Toutefois, il y va de la sécurité et de l’intégrité de tous les renseignements judiciaires. Puisque le Conseil propose que les juges formulent ou approuvent toutes les normes et politiques les concernant, il serait plus facile d’atteindre cette conformité, même en l’absence d’un mécanisme d’application direct.

31. Il est indéniable que si un seul utilisateur – qu’il s’agisse ou non d’un juge – omet d’observer une norme de sécurité appropriée, cela risque de compromettre l’ensemble du réseau ainsi que la sécurité des renseignements judiciaires de tous les juges et des autres utilisateurs du réseau. Par exemple, si un seul juge choisit un mot de passe faible ou omet de chiffrer convenablement un document de nature délicate joint à un courriel (comme un projet de jugement), une personne de l’extérieur non autorisée pourrait obtenir accès non seulement aux dossiers du juge imprudent, mais aussi à ceux des juges qui accordent la plus haute importance à la sécurité de leurs renseignements. C’est pourquoi le Conseil encourage tous les juges et les autres utilisateurs du système judiciaire à adopter les politiques et pratiques énoncées dans le présent document, non seulement dans l’intérêt de l’appareil judiciaire, mais également pour les tierces parties dont les renseignements nécessitent une protection spéciale en vertu de la loi.

32. Dans certains cas où les autorités provinciales ont demandé aux juges de respecter des règles gouvernementales sur la sécurité ou des politiques d’utilisation acceptable, les juges ont soutenu que leur indépendance risquait d’être compromise. Il est souhaité qu’il sera plus facile pour les juges de se conformer aux recommandations énoncées dans le Plan d’action, étant donné qu’il s’agit d’un document rédigé par des juges à l’intention des juges et approuvé en fin de compte par le Conseil canadien de la magistrature ainsi que par d’autres organisations regroupant des juges, comme l’Association canadienne des juges des cours supérieures et l’Association canadienne des juges des cours provinciales.

Structure

33. La structure du Plan d'action suit généralement celle du Manuel du CST. Cependant, contrairement au Manuel du CST, le Plan d'action énonce des politiques précises qui sont approuvées par le Conseil.

Les politiques figurent dans des cases semblables à celle-ci au début de chaque section.

34. Chacun des énoncés de politique est suivi de commentaires concernant la politique et, dans certains cas, d'exemples de lignes directrices que chaque cour peut adopter selon les résultats de sa propre évaluation des risques. Les politiques énoncées dans le Plan d'action se veulent impératives. Les lignes directrices ne sont pas impératives; elles sont proposées à titre indicatif et elles nécessiteront peut-être des modifications pour les adapter à la situation particulière de chaque cour.

35. Afin d'aider davantage les juges et les administrateurs judiciaires à mettre en œuvre le Plan d'action, le présent document comporte aussi de nombreux renvois au Manuel du CST, à un ouvrage fouillé de Charles Wood qui renferme des centaines de modèles de politiques (Wood)[10], ainsi qu'à la norme ISO 17799.

36. En ce qui a trait à la gestion de la sécurité informatique, une grande partie des aspects qui s'appliquent à tout ministère gouvernemental ou organisme du secteur privé s'appliquent également à l'environnement judiciaire. La gestion des renseignements et des utilisateurs ainsi que les mesures de protection opérationnelles et techniques suscitent les mêmes questions. Dans la mesure où ces principes, politiques et procédures génériques s'appliquent à un environnement judiciaire, le Conseil s'est basé sur les normes existantes.

37. Le Plan d'action comporte un glossaire de certains termes et acronymes afin de faciliter la lecture du document pour les profanes.

38. Le Conseil s'est également largement inspiré d'un autre document qui a été adopté pour les cours du Texas le 14 décembre 2001 et qui est intitulé « Judicial Standards for Information Security and Protection ». Ce document est accessible sur le Web à l'adresse http://www.courts.state.tx.us/jcit/index.asp. Le Conseil remercie à cet égard le Texas Judicial Committee on Information Technology (JCIT), qui l'a autorisé à citer librement des extraits de ce document. Le Plan d'action a été élaboré par le Sous-comité de la sécurité informatique du

---

[10] Information Security Policies Made Easy, par Charles Cresson Wood. Publié par Information Shield, 2005. ISBN n° 1-881585-13-1. Http://www.amazon.com/gp/product/1881585131/qid=1152494347/sr=1-11/ref=sr_1_11/102-6265597-7699340?s=books&v=glance&n=283155. Tous les renvois concernent la 10e édition.

Comité consultatif sur la technologie (CCT). Les membres du sous-comité sont les suivants : la juge Fran Kiteley (présidente du sous-comité), la juge Adelle Fruman (présidente du CCT), le juge en chef adjoint Jeffrey Oliphant, M^{me} Jennifer Jordan et M. Martin Felsky. Le sous-comité tient à remercier M^{me} Jeannie Thomas, ancienne directrice exécutive du Conseil, et M^{me} Caroline Collard, conseillère principale, de leur aide très précieuse.

39. Divers organismes, gouvernements, cours et individus ont contribué à l'amélioration des premières ébauches du Plan d'action grâce à l'examen qu'ils en ont fait de même qu'aux commentaires et suggestions qu'ils ont formulés. Le Conseil leur en est reconnaissant.

Note au sujet de la deuxième édition

40. Encore une fois, le Sous-comité de la sécurité informatique du CCT est redevable aux personnes des diverses cours du pays qui ont eu l'amabilité de commenter le Plan d'action. Les membres actuels du sous-comité sont les suivants : la juge Margaret Larlee (présidente du CCT), la juge Janet Simmons (présidente du sous-comité), le juge en chef adjoint Jeffrey Oliphant, la juge Adelle Fruman, le juge Eric Bowie, M^{me} Jennifer Jordan et M. Martin Felsky.

Section 1 : Mesures de protection de gestion

41. Dans quelque organisation que ce soit, toutes les mesures de sécurité débutent et se terminent par la gestion. Dans le cas des cours, cette réalité se traduit le plus souvent par une approche concertée dans le cadre de laquelle les juges énoncent les politiques concernant les renseignements judiciaires, tandis que les administrateurs mettent en oeuvre ces politiques au moyen de mesures opérationnelles et techniques. Le Conseil estime que la responsabilité de *l’élaboration des politiques* concernant la sécurité des renseignements judiciaires est une fonction judiciaire qui ne peut être déléguée à des personnes autres que des juges. La présente section du Plan d’action porte sur le rôle de l’agent de la sécurité informatique du système judiciaire, sur les politiques et la planification, sur la sensibilisation et la formation en matière de sécurité ainsi que sur l’évaluation des menaces et des risques.

1. Agent de la sécurité informatique du système judiciaire

Politique 1 : Chaque juridiction doit veiller à ce qu'un agent de la sécurité informatique du système judiciaire responsable envers la magistrature soit nommé et chargé de surveiller la gestion des mesures de sécurité relatives aux technologies de l'information des cours.

Commentaires

42. La désignation d'un agent de la sécurité informatique du système judiciaire vise à faire en sorte que la sécurité informatique devienne une priorité pour les cours. C'est l'une des principales recommandations (5d) que le Conseil a approuvée le 30 novembre 2001 (voir l'annexe 1). Elle devrait également permettre de veiller à ce que la situation et les besoins uniques du monde judiciaire constituent une partie intégrante de la planification de la sécurité informatique et de la conception des systèmes. L'agent de la sécurité informatique du système judiciaire peut agir en qualité d'agent de liaison technique avec le personnel affecté à l'administration des systèmes informatiques afin de mieux sensibiliser les utilisateurs judiciaires aux questions de sécurité. Le Conseil estime qu'au moins une personne haut placée de chaque juridiction devrait être responsable exclusivement envers la magistrature en ce qui a trait à la sécurité informatique des renseignements judiciaires. (Voir la norme ISO 17799, section 6.)

43. La principale recommandation est que chaque juridiction nomme un agent de la sécurité informatique du système judiciaire, dont les qualifications et les fonctions sont énoncées dans le Plan d'action. L'agent de la sécurité informatique du système judiciaire devrait être un spécialiste en technologies de l'information qui possède de l'expérience technique et une bonne connaissance des protocoles de sécurité qui conviennent à la taille et à la complexité du système informatique de la cour. Cette personne doit être nommée à un poste de niveau de gestion, elle doit être capable de représenter la magistrature à l'égard de la sécurité informatique et elle doit relever du juge en chef.

44. L'agent de la sécurité informatique du système judiciaire serait responsable de fournir à la magistrature des avis impartiaux sur toutes les questions concernant la sécurité de l'informatique et d'effectuer vérifications périodiques de la sécurité des systèmes informatiques qui contiennent des renseignements judiciaires. De plus, l'agent de la sécurité informatique du système judiciaire aurait la responsabilité générale des questions de sécurité informatique qui relèvent principalement de la magistrature, notamment l'élaboration des politiques, l'évaluation des risques et la surveillance de la conformité aux politiques et normes telles que le Plan d'action et la norme ISO 17799.

45. Habituellement, les juges ne gèrent pas les systèmes d'information qu'ils utilisent, mais partagent plutôt l'accès aux systèmes que leur fournit la province. En conséquence, ils doivent prendre en main les questions de sécurité en collaboration avec les organismes chargés de la gestion des réseaux qu'ils utilisent. La nomination d'un agent de la sécurité informatique du système judiciaire vise à faciliter cette collaboration en permettant aux juges d'avoir accès à un conseiller et représentant ayant la formation voulue.

46. Le chapitre 3 du Manuel du CST comporte une description des différents rôles et responsabilités liés à la sécurité informatique en matière organisationnelle. De l'avis du Conseil, chaque cour devrait avoir son propre agent de la sécurité informatique du système judiciaire qui serait responsable envers la magistrature, mais cette fonction peut être greffée à d'autres responsabilités, à condition qu'il n'y ait pas de conflit avec celles-ci. (Par exemple, la même personne ne pourrait pas agir à la fois comme agent de la sécurité informatique du système judiciaire et comme agent de la sécurité des renseignements pour le compte de l'administration judiciaire.) À l'instar du coordonnateur de procès, l'agent de la sécurité informatique du système judiciaire peut travailler à l'emploi du procureur général, mais il doit relever seulement du juge en chef. En général, les facteurs suivants devraient s'appliquer :

    - L'agent de la sécurité informatique du système judiciaire traitera principalement de questions de politique, de planification, de normes ainsi que de l'examen et de la vérification de la mise en oeuvre de la politique en matière de sécurité. La fonction requiert de l'expérience et des connaissances tant au niveau de la sécurité qu'au niveau des technologies de l'information.

    - L'agent de la sécurité informatique du système judiciaire devrait être responsable envers la magistrature par l'entremise du juge en chef.

    - L'agent de la sécurité informatique du système judiciaire devrait être sensible à la question de l'indépendance judiciaire.

47. Les tâches de l'agent de la sécurité informatique du système judiciaire peuvent varier selon les systèmes informatiques de chaque cour, mais le Conseil recommande que cette personne soit chargée des grandes responsabilités suivantes :

    - élaborer les politiques en matière de sécurité en vue de les soumettre à l'approbation des juges;

    - conseiller les juges et les administrateurs au sujet des préoccupations relatives à la sécurité informatique en ce qui concerne les renseignements judiciaires;

- surveiller de façon générale l'adoption et la mise en œuvre du Plan d'action et des autres normes pertinentes en matière de sécurité informatique du système judiciaire;
- coordonner l'interaction liée à la sécurité à l'intérieur de la cour et entre celle-ci et d'autres organismes comme le Conseil et le CMF, ainsi qu'avec les organismes provinciaux et fédéraux correspondants qui sont responsables de la sécurité informatique;
- concevoir et offrir des programmes de sensibilisation et de formation en matière de sécurité à l'intention des utilisateurs judiciaires et en assurer la coordination avec des organismes de l'extérieur (notamment le partenariat formé entre l'INM et le CMF);
- planifier et surveiller, en collaboration avec le chef de l'exploitation des systèmes informatiques, des évaluations et vérifications régulières des menaces et des risques ainsi que des contrôles d'assurance réguliers pour la cour conformément aux politiques judiciaires;
- se tenir au courant des nouveaux risques liés à la sécurité des renseignements et diffuser les renseignements à ce sujet à l'intérieur de la cour;
- surveiller le respect des Lignes de conduite sur la surveillance informatique;
- valider et vérifier le processus d'élimination des métadonnées de la cour;
- organiser des vérifications ponctuelles de la sécurité informatique de la cour;
- rédiger des règles concernant le système de détection d'intrusion (SDI) et la surveillance de celui-ci;
- surveiller régulièrement l'utilisation des outils SDI en version réseau afin de garantir qu'ils fonctionnent comme prévu;
- établir des liens avec les organismes responsables de répondre aux incidents et avec les agents de la sécurité informatique du système judiciaire des autres cours et échanger quant aux menaces, vulnérabilités et incidents pertinents découverts;
- surveiller le processus d'approbation des nouvelles applications fournies aux utilisateurs judiciaires ou demandées par ceux-ci;
- veiller à ce que tous les utilisateurs aient une formation convenable à l'égard de l'utilisation de la technologie de chiffrement;
- surveiller la mise en œuvre de la technologie de chiffrement à l'intention des utilisateurs judiciaires.

2. Politique et planification

Politique 2 : La planification relative à la sécurité des technologies de l'information et l'élaboration de politiques visant à assurer la protection des renseignements judiciaires sont des fonctions judiciaires. La magistrature doit prendre la responsabilité de l'élaboration des politiques qui touchent les utilisateurs judiciaires ou la façon dont ils exercent leurs fonctions. Toutes les politiques des cours en matière de sécurité doivent être interprétées et appliquées conformément aux Lignes de conduite sur la surveillance informatique du Conseil.

Commentaires

48. Les politiques relatives à la sécurité des renseignements renvoient à l'ensemble de règles, protocoles et pratiques que les juges et cours suivent afin de gérer et de protéger leurs renseignements. Voir la norme ISO 17799, section 5 « Security Policy ».

49. Les politiques peuvent être mises en oeuvre de différentes façons. Le lecteur trouvera des commentaires intéressants à ce sujet ainsi que des modèles au chapitre 5 du Manuel du CST.

50. Le présent Plan d'action couvre trois types de politiques :

- les *politiques de programme* établissent le programme de sécurité inhérent au système informatique d'une cour. Elles constituent un document de haut niveau qui est exhaustif et ne nécessite habituellement pas de mises à jour fréquentes. Ce type de politiques s'applique indépendamment de la nature du matériel ou du logiciel qu'utilise la cour et elles sont impératives;

- les *politiques propres à un système* énoncent les règles et pratiques servant à protéger un système d'information donné. Ces politiques couvrent uniquement le ou les systèmes concernés et peuvent être modifiées en fonction des changements touchant le système ou encore la fonctionnalité ou les vulnérabilités de celui-ci. Ainsi, les cours qui utilisent le système d'exploitation de réseau Novell Netware auront besoin de règles différentes de celles qui emploient les systèmes d'exploitation Windows de Microsoft;

- les *politiques propres à une question* portent sur des questions ponctuelles qui intéressent ou préoccupent la cour. Ces types de politiques ont habituellement une portée restreinte et particulière et sont fréquemment modifiées. Leur élaboration peut être déclenchée par un incident lié à la sécurité informatique. Ainsi, la politique d'une cour concernant l'utilisation acceptable du courriel est une politique propre à une question.

Politiques de programme

51. Les politiques de programme s'appliquant aux juges doivent prendre en compte le cadre législatif et réglementaire ainsi que les règles administratives canadiennes et elles doivent également être fondées sur les fonctions et la structure organisationnelle de la cour. L'élaboration et la promulgation des politiques de programme relèvent du juge en chef de chaque cour. L'agent de la sécurité informatique du système judiciaire jouerait un rôle clé dans l'élaboration de ces politiques, dont la mise en oeuvre ne pourrait avoir lieu que dans le cadre d'une consultation avec l'autorité administrative concernée de la cour.

Politiques propres à un système

52. Certaines cours auront probablement de nombreux ensembles de politiques propres à leurs systèmes en matière de sécurité, qu'il s'agisse de politiques très générales (p. ex., règles relatives au contrôle d'accès qui concernent les personnes pouvant avoir des comptes d'utilisateur) ou de règles très précises (p. ex., autorisations du système traduisant une séparation des tâches entre les membres du personnel qui s'occupent du traitement des renseignements relatifs aux instances). Toutes les politiques propres à un système doivent être compatibles avec la politique de programme. Dans bien des cas, les rédacteurs de ces politiques doivent posséder des connaissances techniques approfondies des systèmes informatiques afin que les politiques propres à un système en question puissent être mises en pratique.

Politiques propres à une question

53. Les énoncés de politique propres à une question peuvent couvrir un vaste éventail de sujets, comme l'accès des utilisateurs à Internet, l'installation de logiciels ou d'équipement non autorisés et la réexpédition de courriels.[11] Les politiques d'utilisation acceptable appartiennent à cette catégorie. Les cours doivent élaborer des politiques qui s'appliquent à tous les utilisateurs lorsque les systèmes contenant des renseignements judiciaires sont partagés. Cependant, seules les politiques approuvées par la magistrature peuvent s'appliquer aux utilisateurs judiciaires. En décembre 2003, le Comité exécutif du Conseil canadien de la magistrature a approuvé un « Modèle de règles d'utilisation acceptable des ordinateurs pour le personnel judiciaire », dont un exemplaire est joint à l'annexe 6 du Plan d'action.

---

[11] Ainsi, les cours souhaiteront peut-être conseiller aux juges de ne pas configurer leur programme de courrier électronique de façon à permettre la réexpédition automatique de leurs messages protégés à une autre adresse par l'entremise d'une connexion non chiffrée, ou encore décider de désactiver la fonction de réexpédition de courriels.

Lignes directrices relatives à l'élaboration des politiques

54. Toutes les politiques relatives à la sécurité des systèmes informatiques devraient être fondées sur l'évaluation que la cour fait des menaces et des risques auxquels elle est exposée et comporter généralement les éléments suivants :

    énoncé de l'objet : l'énoncé de l'objet explique la raison pour laquelle la politique est établie et les buts qu'elle vise à atteindre en matière de sécurité des technologies de l'information;

    description de la portée : la description de la portée fait état des ressources de la cour que couvre la politique, soit le matériel, le logiciel (systèmes d'exploitation, applications et communications), les données, le personnel, les installations et l'équipement périphérique (y compris l'équipement de télécommunications);

    description de la répartition des responsabilités : l'énoncé de politique comporte une description des responsabilités relatives à la gestion du programme de sécurité, y compris les rôles respectifs du juge en chef ou d'autres juges, de l'agent de la sécurité informatique du système judiciaire, des utilisateurs judiciaires, des administrateurs des cours et de tous les autres utilisateurs;

    description de la mise en oeuvre : l'énoncé de politique comporte une description de la façon dont la cour surveillera la mise en oeuvre et l'application de la politique;

    mention de la date de révision : l'énoncé de politique indique la date à laquelle la cour a l'intention de revoir la politique en question.

55. Les politiques doivent être rédigées de façon à en permettre la compréhension par tous les utilisateurs.

56. Toutes les politiques en matière de sécurité devraient faire l'objet de discussions avec les juges nouvellement nommés et être décrites lors des séances d'information à l'intention du nouveau personnel ainsi que dans le cadre d'une formation régulière à la sensibilisation en matière de sécurité informatique.

57. Les entrepreneurs, consultants et instructeurs de l'extérieur devraient être tenus de signer des accords de sécurité ou de confidentialité dans lesquels ils reconnaissent qu'ils sont au courant de leurs responsabilités et qu'ils se conformeront aux politiques de la cour en matière de sécurité. Le Plan d'action ne traite pas des cas où toutes les fonctions informatiques d'une cour sont imparties à une tierce partie, étant donné que cela nécessiterait un examen plus complexe des questions concernant les politiques d'intérêt public. Voir la norme ISO 17799, section 6.2.

58. Des politiques propres aux systèmes devraient être adoptées à l'égard de programmes majeurs comme les systèmes d'exploitation, les applications du courriel et les progiciels de bureautique.

59. Des politiques propres aux questions dont la rédaction serait confiée à des juges devraient être adoptées en ce qui concerne, notamment, l'utilisation acceptable d'Internet et du courriel, l'installation des logiciels et l'utilisation personnelle des ressources informatiques. Lorsque les utilisateurs judiciaires ouvrent une session, un avis indiquant que l'utilisation de l'ordinateur est assujettie à ces politiques établies par les juges devrait être clairement affiché.

60. Il y a lieu de réviser les politiques relatives à la sécurité chaque année afin de s'assurer qu'elles sont à jour et qu'elles sont conformes au système informatique et à l'environnement judiciaire courants. Il est recommandé d'effectuer un examen indépendant de temps à autre. (Voir la norme ISO 17799, section 15.)

3. Sensibilisation et formation en matière de sécurité

Politique 3 : Les cours doivent offrir à tous les utilisateurs une formation continue en matière de sensibilisation à la sécurité informatique ainsi que de la documentation connexe, et tous les membres du personnel informatique qui utilisent des renseignements judiciaires dans le cadre de leur travail doivent obligatoirement suivre une formation approfondie en matière de sécurité informatique.

Commentaires[12]

61. La sensibilisation ainsi que la formation et l'éducation à la sécurité sont toutes nécessaires pour assurer le succès de tout programme relatif à la sécurité des renseignements. Ces trois éléments sont liés entre eux, mais ils mettent en cause des niveaux d'apprentissage foncièrement différents.

Sensibilisation à la sécurité

62. Les programmes de sensibilisation à la sécurité visent à attirer l'attention sur la sécurité. Les programmes de cette nature devraient être bien établis au sein de la cour. À titre d'exemple, chaque utilisateur du système devrait recevoir de la documentation qui explique la nécessité de la sécurité informatique et la responsabilité des utilisateurs pour garantir cette sécurité.

63. La sensibilisation à la sécurité constitue le point de départ de l'acquisition de connaissances en matière de sécurité pour tous les utilisateurs, quels que soient leurs fonctions ou leurs tâches. Le niveau de base de sensibilité à la sécurité qui est exigé des étudiants d'été ou des aides commis est le même que celui qui est nécessaire dans le cas des juges principaux et des gestionnaires des cours. Les programmes de sensibilisation à la sécurité informatique devraient être liés directement à l'élaboration des politiques en matière de sécurité.

64. Dans le cadre de sa responsabilité de se tenir au courant des nouveaux risques en matière de sécurité, l'agent de la sécurité informatique du système judiciaire devrait surveiller les sources pertinentes, comme les sites des fournisseurs et les sites relatifs à la sécurité, afin de veiller à ce que les utilisateurs sachent comment détecter ou prévenir les incidents touchant la sécurité informatique du système judiciaire.

---

[12] Voir Wood, section 6.02, et la norme ISO 17799, section 8.

Formation et sensibilisation

65. La formation et la sensibilisation visent à promouvoir la compréhension des aspects liés à la sécurité des systèmes et applications informatiques utilisés. Ainsi, tous les utilisateurs doivent connaître les éléments de sécurité du logiciel de traitement de texte de leur ordinateur et savoir comment sauvegarder les renseignements contenus dans leur ordinateur. Ils doivent également comprendre les éléments de sécurité du réseau local auquel ils sont reliés ainsi que les problèmes de sécurité liés à la connectivité à Internet. Il se peut que certaines questions se chevauchent, mais chaque système est une composante distincte qui nécessite son propre ensemble de mesures de sécurité. La formation et la sensibilisation en matière de sécurité informatique tiennent compte du caractère unique de chaque système d'exploitation et de chaque application.

66. Des cours de formation et de sensibilisation en matière de sécurité devraient être offerts à tous les utilisateurs qui ont accès à des renseignements judiciaires. Il est souhaitable d'offrir périodiquement (au moins une fois l'an) des cours de recyclage axés sur la sensibilisation à la sécurité.

67. Une formation structurée en matière de sécurité informatique devrait être offerte à tous les nouveaux utilisateurs lors de leur séance d'orientation. Les utilisateurs devraient recevoir une formation continue en matière de sécurité sous forme de bulletins, de ressources en direct, d'avertissements, de conseils ou de notes, ainsi qu'une formation annuelle complémentaire. L'ensemble de la formation et de la documentation relative à la sécurité informatique devrait être coordonnée dans la mesure du possible et correspondre avec celle qui est offerte aux juges par l'entremise d'organisations de la magistrature comme l'Association canadienne des juges de cours provinciales et le Partenariat de formation informatisée entre l'Institut national de la magistrature et le Bureau du Commissaire à la magistrature fédérale.

Éducation

68. L'éducation diffère de la formation au plan de l'éventail et de la profondeur des connaissances et aptitudes acquises. L'éducation en matière de sécurité, y compris les cours formels et les programmes d'accréditation, est tout indiquée pour l'agent de la sécurité informatique du système judiciaire et le personnel chargé des aspects administratifs des systèmes informatiques.

69. Les administrateurs et le personnel affectés à la gestion des réseaux et des pare-feux ainsi que les gestionnaires des aspects techniques des réseaux devraient recevoir une formation précise sur l'exploitation des produits de sécurité utilisés dans leur environnement afin de mieux pouvoir régler les problèmes liés à la sécurité informatique.

70. Les administrateurs de réseau devraient être tenus de réussir un test formel sur les questions de sécurité précises liées aux systèmes matériels et logiciels dont ils sont responsables.

4. Évaluation des menaces et des risques

Politique 4 : Chaque cour doit planifier et effectuer régulièrement une évaluation des menaces et des risques (EMR). Le niveau de détail, l'ampleur et la fréquence de l'EMR varieront selon le niveau de risque.

Commentaires

71. La sécurité représente dans tous les cas un compromis.[13] Les mesures de sécurité peuvent être coûteuses et difficiles à mettre en oeuvre et tout organisme doit faire preuve de discipline pour respecter son engagement envers la sécurité. Il est important que les mesures prises pour protéger les renseignements judiciaires constituent une réponse efficace aux menaces pertinentes tout en étant proportionnées aux risques.

72. Les menaces à la sécurité, à l'intégrité et à l'accessibilité des renseignements judiciaires proviennent de différentes sources qui sont parfois classées comme suit :

[13] [TRADUCTION] « Étant donné que certaines mesures de contrôle de la sécurité informatique freinent la productivité, les mesures de sécurité représentent habituellement un compromis visant à permettre aux praticiens de la sécurité, aux utilisateurs des systèmes ainsi qu'au personnel chargé de l'exploitation et de la gestion de ceux-ci d'atteindre un équilibre satisfaisant entre la sécurité et la productivité », Harold F. Tipton et Micki Krause, *Handbook of Information Security Management*, http://www.ccure.org/Documents/HISM/003-006.html.

Type de menace	Exemple
Menaces naturelles, y compris la foudre et les incendies, orages, inondations, températures extrêmes ou autres catastrophes naturelles.	Une surtension provoquée par la foudre met le serveur de fichier hors d'état; le système ne fonctionne plus et personne ne peut entrer dans le système pour vérifier son courriel, réviser des documents ou exécuter d'autres tâches informatiques.
Menaces délibérées provenant de personnes de l'extérieur comme des pirates informatiques, des terroristes, des membres du crime organisé, des activistes politiques ou des parties à un litige mécontentes.	Un jeune modifie le texte d'un jugement en ligne en sabotant le serveur Web de la cour. Un employé contractuel en informatique obtient accès aux projets de jugement stockés sur une bande de sauvegarde et les affiche sur un site Web. Un juge ouvre un courriel et répand un virus qui immobilise le service de courrier électronique de la cour pendant 48 heures. Un juge se fait voler son ordinateur portatif à bord de son véhicule, lequel était garé dans le stationnement intérieur d'un immeuble du centre-ville. L'ordinateur renferme des renseignements personnels concernant un jeune contrevenant, les transcriptions d'un interrogatoire préalable qui font l'objet d'une interdiction de publication ainsi que les noms, adresses postales, numéros de téléphone et adresses électroniques de sept juges.
Menaces délibérées ou accidentelles de la part d'administrateurs et d'utilisateurs du système.	Un employé mécontent envoie des messages haineux à des politiciens en utilisant l'adresse électronique d'un juge. Un juge écrase par inadvertance la version finale d'un jugement de 150 pages qui devait être communiqué le jour même. Trois bandes de sauvegarde sont manquantes; des renseignements critiques concernant l'établissement du calendrier de la cour ne peuvent être récupérés et tout le travail de calcul et d'entrée des données doit être refait.
Panne d'équipement, problème mécanique, erreur logicielle ou toute autre défaillance technique.	La tête de lecture-écriture du lecteur de disque dur du serveur fait défaut. Le système ne peut être utilisé avant qu'une autre tête soit installée et que toutes les copies de sauvegarde soient restaurées.

73. Sans l'adoption de mesures de protection efficaces, les utilisateurs sont vulnérables à ces attaques et à de nombreuses autres. Voici des exemples de mauvaises pratiques liées à la sécurité des renseignements :

- omission de déceler les erreurs et d'appliquer en temps opportun les sous-programmes de correction liés à la sécurité;
- formation insuffisante du personnel responsable en ce qui a trait à la sécurité du réseau;
- insuffisance de la sensibilité à la sécurité informatique dans l'ensemble de la cour;
- envoi de données non chiffrées sur les réseaux publics de courrier électronique, comme MSN Hotmail;
- utilisation répandue de mots de passe faibles qu'il n'est pas obligatoire de modifier régulièrement;
- absence de politiques et de procédures concernant la sécurité des renseignements judiciaires;
- insuffisance de la sécurité matérielle entourant les ressources informatiques, comme les ordinateurs portatifs ;
- sauvegarde insuffisante des renseignements judiciaires, notamment ceux qui se trouvent sur les ordinateurs personnels et les disquettes;
- protection insuffisante contre les virus.

74. Pour que la planification relative à la sécurité soit efficace, il est nécessaire de procéder à une évaluation des menaces et des risques (EMR). Il s'agit d'une démarche formelle qui devrait être faite à fond et guidée par des spécialistes en matière de sécurité informatique.[14] Étant donné que l'environnement informatique est différent d'une cour à l'autre et que les préoccupations concernant la sécurité diffèrent même parmi les juges informés, chaque cour doit procéder à une EMR adaptée à sa propre situation. En général, les étapes d'une EMR sont les suivantes :

---

[14] Pour obtenir des renseignements utiles au sujet de la planification et de la mise en oeuvre d'une EMR, il y a lieu de consulter une publication technique de la GRC datée de novembre 1994 et intitulée « Guide d'évaluation de la menace et des risques pour les technologies de l'information ». Pour des mises à jour, voir le site Web de la GRC à http://www.rcmp-grc.gc.ca et le site Web du CST à www.cse-cst.gc.ca. Le lecteur trouvera également d'excellents commentaires à ce sujet au chapitre 7 du Manuel du CST.

Inventaire des biens : au cours de cette étape, tous les biens (y compris les renseignements, le matériel et les logiciels) qui nécessitent une protection sont identifiés, qu'ils se trouvent à la cour ou au domicile des utilisateurs. Dans le cas d'une cour, les renseignements détenus comprennent non seulement les produits des travaux judiciaires, mais également l'information obtenue de tierces parties ou à leur sujet (p. ex., les renseignements obtenus par écoute électronique ou les renseignements qui concernent des jeunes contrevenants et qui peuvent être assujettis à des exigences légales en matière de sécurité).

Évaluation des menaces : cette mesure consiste, pour chaque bien, à déterminer et à évaluer toutes les menaces, y compris leur source et leur type, la probabilité qu'elles se concrétisent et l'impact qu'elles pourraient avoir.

Évaluation des risques : il s'agit ici de vérifier jusqu'à quel point les dispositifs et mesures existants sont susceptibles d'assurer une protection efficace contre les menaces identifiées, c'est-à-dire d'évaluer les vulnérabilités des systèmes de la cour en ce qui a trait à la sécurité et le degré *réel* de risque associé à chaque menace.

75. Lorsque toutes les étapes d'une EMR sont terminées, le résultat donne lieu à une évaluation des risques possibles. Le tableau qui suit présente un exemple de calcul découlant de cette évaluation. Grâce à ce calcul, il est plus facile pour les cours de déterminer les méthodes à utiliser afin de mieux protéger les renseignements judiciaires.

Tableau présentant un exemple de calcul découlant d'une EMR

Description des menaces	Impact possible de la menace (1-3)	Probabilité que la menace se concrétise (1-3)	Évaluation des risques (produit de l'impact possible par la probabilité)
1. Un pirate obtient accès à des ressources internes privées.	Élevé – 3	Moyenne – 2	6
2. Un utilisateur mécontent obtient accès non autorisé à des renseignements, ce qui donne lieu à la modification ou à la divulgation de renseignements sensibles.	Élevé – 3	Élevée – 3	9
3. Un virus s'infiltre dans le système de la cour et endommage des renseignements critiques.	Moyen – 2	Élevée – 3	6
4. Par suite d'une catastrophe naturelle, des données sont perdues et le système ne peut être utilisé.	Élevé – 3	Moyenne – 2	6
5. Un juge endommage par inadvertance des renseignements critiques.	Élevé – 3	Moyenne – 2	6
6. Un dispositif du matériel est défectueux, ce qui entraîne la perte de données.	Moyen – 2	Moyenne – 2	4

Section 2 : Mesures de protection opérationnelles

76. Les mesures de protection opérationnelles appuient la mise en oeuvre des politiques en matière de sécurité en mettant l’accent sur le comportement de l’utilisateur et l’application de pratiques exemplaires. De nombreuses mesures opérationnelles importantes ne sont pas traitées dans le Plan d’action, parce qu’elles ne concernent pas directement le milieu judiciaire. La présente section du Plan d’action traite de trois aspects clés qui intéressent particulièrement les juges : la sauvegarde, la sécurité matérielle et la classification des renseignements judiciaires. Pour obtenir un point de vue beaucoup plus large et informatif au sujet des mesures de protection opérationnelles, il y a lieu de consulter la partie III du Manuel du CST.

5. Sauvegarde et planification de la continuité des opérations

Politique 5 : Les cours doivent protéger les renseignements judiciaires en cas de catastrophe ou de défaillance du système et fournir un degré élevé d'assurance que le service interrompu par suite d'un tel événement sera rétabli dans les meilleurs délais. Les utilisateurs judiciaires doivent avoir accès au stockage réseau et le contenu de celui-ci doit être sauvegardé au moins une fois par jour. Des dispositions efficaces doivent être prises en vue de faciliter la sauvegarde des renseignements judiciaires créés ou reçus et stockés localement, par exemple sur des ordinateurs portatifs pendant les déplacements.

Commentaires[15]

77. La ***sauvegarde*** consiste à copier régulièrement les renseignements critiques concernant le système et la configuration ainsi que les documents afin d'en assurer la disponibilité en cas de perte des renseignements se trouvant sur les serveurs et les postes de travail. Lorsqu'un document est effacé par inadvertance ou qu'un programme est corrompu, il suffit souvent de quelques heures pour restaurer dans le serveur des copies de sauvegarde qui sont habituellement stockées dans des bandes magnétiques de grande capacité.

78. La ***planification de la continuité des opérations*** vise à protéger le système en cas de panne. Ainsi, lorsqu'un serveur est endommagé ou perdu, la cour devrait pouvoir le remplacer rapidement par un système entièrement fonctionnel dans lequel les fichiers et les applications pourraient être restaurés. Toutes les cours devraient établir un processus formel de planification de la continuité des opérations.

79. La présente section comporte une description de différents éléments clés des plans de continuité des opérations et des procédures de sauvegarde.

Sauvegarde

80. Les renseignements judiciaires devraient être stockés et sauvegardés de façon à ce que les utilisateurs judiciaires y aient un accès exclusif. Les copies de sauvegarde devraient ensuite être archivées conformément à la politique de la cour. (Voir la rubrique « Classification des renseignements judiciaires », ci-dessous.)

81. Afin de faciliter la sauvegarde des données des postes de travail locaux et ordinateurs portatifs, il est préférable d'enregistrer les renseignements judiciaires de manière uniforme dans des fichiers désignés, par exemple : « C:\Documents\Judiciaires\ ».

---

[15] Voir Wood, sections 8.04.01 et 11, et la norme ISO 17799, sections 10 et 14.

82. Lorsque les systèmes assurant périodiquement la sauvegarde réseau ne permettent pas la saisie des données des postes de travail, il convient de rappeler aux utilisateurs judiciaires de sauvegarder régulièrement les renseignements contenus dans leur ordinateur a) en copiant les renseignements judiciaires dans le lecteur réseau désigné ou b) en copiant le contenu du dossier local désigné sur un support amovible fiable comme un CD ou un DVD inscriptible.

83. Les bandes de sauvegarde de réseau qui contiennent des renseignements judiciaires doivent être protégées par chiffrement et rangées hors des lieux dans un endroit sûr et fiable. Lorsqu'elles sont faites séparément, les copies de sauvegarde des renseignements des postes de travail locaux devraient être gardées dans une armoire verrouillée.

84. Les procédures de sauvegarde et de rotation régulières devraient comprendre des sauvegardes hebdomadaires « complètes » et des sauvegardes « incrémentielles » tous les soirs pour tous les systèmes d'informatique et d'exploitation de réseau, les programmes d'application et les fichiers de données. Les sauvegardes complètes couvrent tous les systèmes, applications et fichiers en cours d'utilisation, tandis que les sauvegardes incrémentielles se limitent aux changements apportés aux systèmes et aux fichiers depuis la dernière sauvegarde.

85. L'accès aux bandes de sauvegarde doit être assujetti aux Lignes de conduite sur la surveillance informatique (voir l'annexe 2).

86. Une procédure doit être mise en oeuvre pour valider et vérifier régulièrement les bandes de sauvegarde afin de s'assurer qu'elles sont lisibles, plus particulièrement avant de les envoyer à l'installation d'entreposage extérieur.

87. Toutes les bandes de sauvegarde doivent être étiquetées correctement.

88. Une copie complète sur support papier de tous les éléments matériels et logiciels (y compris les données relatives aux systèmes d'exploitation, aux applications et aux éléments matériels et logiciels achetés ainsi que le nom du vendeur et le nom de la cour pour chaque élément matériel et logiciel) devrait être conservée à l'installation d'entreposage extérieure des bandes et régulièrement mise à jour.

89. Au moins une copie complète sur support papier du plus récent plan de continuité des opérations ainsi que des polices d'assurance informatique (à utiliser en cas de perte d'un système informatique) devrait également être conservée à l'installation où sont entreposées les bandes hors des lieux.

90. Des copies papier et des versions numériques des configurations de système standard ainsi que de la documentation se rapportant à toutes les applications critiques devraient être conservées dans une installation d'entreposage sûre hors des lieux.

91. Il y a lieu de conserver les bandes stockées à l'installation d'entreposage extérieure dans des contenants appropriés à l'épreuve de la poussière et de les disposer sur le côté (surtout les bandes de neuf pistes) afin d'éviter l'altération ou la perte des données.

92. Il est nécessaire de vérifier chaque année les bandes d'archivage (celles qui sont conservées pendant deux ans ou plus) pour s'assurer qu'elles sont lisibles et d'en restaurer le contenu sur un support plus neuf tous les deux ou trois ans afin que la capacité de restauration demeure intacte (surtout lorsque les anciennes bandes deviennent illisibles par suite de l'acquisition de nouveaux éléments matériels ou logiciels en raison de nouvelles configurations des données en mode texte ou point).

93. L'archivage des renseignements judiciaires, y compris les cahiers d'audience électroniques, doit être fait conformément aux politiques établies par les juges.

Continuité des opérations

94. La cour devrait périodiquement mettre à jour ses plans de continuité des opérations et les mettre à l'épreuve régulièrement afin que tous les systèmes contenant des renseignements judiciaires soient disponibles en cas de perte majeure.

95. Si des mesures de protection satisfaisantes sont en place, la cour devrait envisager la possibilité de conclure une entente relative à l'utilisation d'une « salle blanche » de rechange avec une entreprise de dépannage informatique publique ou privée, afin de prévoir un emplacement pour la reconstruction des systèmes informatiques et la réinstallation des données en cas de catastrophe ou de défaillance.

96. En ce qui concerne ses systèmes les plus critiques, la cour pourrait envisager la possibilité de conclure une entente relative à l'utilisation d'un « site branché » de rechange avec une entreprise de dépannage informatique publique ou privée, afin de pouvoir reconstruire rapidement ses systèmes et données informatiques en cas de catastrophe ou de défaillance. L'entreprise offrant le « site branché » posséderait des éléments matériels et logiciels compatibles avec ceux que la cour utilise tous les jours. En cas de défaillance, les ordinateurs du « site branché » pourraient être utilisés.

97. S'il n'est pas possible de conclure des ententes relatives à l'utilisation d'un « site branché » ou d'une « salle blanche », les ordinateurs de bureaux de même que les logiciels peuvent être remplacés en effectuant des achats pour pallier la situation d'urgence immédiatement après la défaillance.

6. Sécurité matérielle

Politique 6 : Tous les éléments critiques de l'équipement de réseautique devraient se trouver dans un environnement à accès contrôlé et limité au personnel responsable de leur administration et de leur maintenance. Le local doit être muni de dispositifs de contrôle de l'environnement satisfaisants. Si les utilisateurs judiciaires se servent d'ordinateurs portatifs, des mécanismes comme des dispositifs de verrouillage et des avertisseurs devraient être fournis et utilisés de façon à réduire les risques de vol. Le chiffrement du disque est fortement recommandé pour tous les ordinateurs portatifs. Des mesures comme la tenue de registres de contrôle d'accès et la surveillance par caméra vidéo de l'équipement de réseautique devraient être mises en oeuvre. Les cours doivent veiller à ce qu'aucun renseignement judiciaire ne puisse être récupéré lorsqu'elles se débarrassent d'un dispositif informatique ou d'un support de données (y compris les rubans magnétiques servant aux sauvegardes).

Commentaires[16]

98. La sécurité matérielle s'entend de la protection des immeubles et de l'équipement (ainsi que des renseignements et logiciels qui s'y trouvent) contre les introductions par effraction, vols, actes de vandalisme, catastrophes naturelles et autres et dommages accidentels. Les gestionnaires doivent accorder une attention particulière à la construction de l'immeuble où se trouvent les systèmes informatiques, à la répartition des articles d'équipement entre les pièces de l'immeuble, aux procédures d'intervention en cas d'urgence, aux règlements régissant l'installation et l'utilisation de l'équipement, à l'approvisionnement en eau et en énergie, à la manutention des produits ainsi qu'aux relations avec le personnel, les entrepreneurs de l'extérieur, les autres cours et les ministères et organismes gouvernementaux. Certaines solutions exigent l'installation de mécanismes de verrouillage, d'extincteurs, de limiteurs sur tension, de barreaux de fenêtre, de détecteurs automatiques d'incendie et de systèmes d'alarme.

99. Les cours devraient s'assurer que tous les appareils et supports servant à stocker des renseignements judiciaires, notamment les disquettes, les CD et les DVD inscriptibles, les disques durs, les bandes de sauvegarde et les dispositifs d'entreposage à semi-conducteur (les unités de mémoire Flash USB), sont détruits physiquement ou nettoyés de manière professionnelle lorsqu'ils sont éliminés à l'extérieur du système judiciaire. Cela comprend aussi les appareils portatifs et les périphériques tels que les téléphones intelligents, les assitants numériques personnels (PDA), les appareils « Blackberry », certaines imprimantes, les photocopieurs numériques, les appareils multifonctionnels et les scanneurs. Il ne suffit pas de

[16] Voir Wood, section 7, et la norme ISO 17799, section 9.

supprimer les fichiers ou de reformater le disque dur pour éliminer toute trace de données pouvant être confidentielles.

100. Les pièces protégées devraient comporter les caractéristiques suivantes :

- des murs pleine hauteur ainsi que des murs et plafonds résistants au feu;
- un maximum de deux portes. Les portes doivent être solides, résistantes au feu, verrouillables et visibles pour le personnel;
- les fenêtres devraient être petites et relativement peu nombreuses et toutes devraient être munies de verrous satisfaisants;
- contrôle des clés : le fait de verrouiller les portes et fenêtres constitue une stratégie efficace en matière de sécurité lorsque les autorités concernées assurent une tenue en bonne et due forme des clés (qu'il s'agisse de clés de métal, de cartes-clés ou d'une combinaison de ces deux types de clés).
- Les supports entreposés sur place, comme les bandes de sauvegarde, devraient être conservés dans des contenants inviolables et résistants au feu.
- Les extincteurs devraient être conservés près de l'équipement et les utilisateurs devraient recevoir la formation nécessaire pour pouvoir les utiliser. L'installation et la recharge des extincteurs devraient être vérifiées chaque année.
- Il est nécessaire d'utiliser une alimentation sans coupure afin de protéger l'équipement informatique critique en cas de panne d'électricité. Des filtres et des limiteurs de surtension visant à contrôler les variations brusques de courant devraient être installés.Si c'est ce que recommande l'EMR, il pourrait être opportun que certains sites soient dotés d'un dispositif d'alimentation électrique de réserve.
- Il y aurait lieu de fournir aux utilisateurs judiciaires qui possèdent des ordinateurs portatifs des mécanismes comme des dispositifs de verrouillage et des avertisseurs qu'ils pourront utiliser afin de réduire les risques de vol. L'utilisation de techniques de chiffrement du disque est fortement recommandée pour tous les ordinateurs portatifs. Il serait également oppurtun d'aviser ces utilisateurs de ne pas laisser leurs ordinateurs sans surveillance ou sans protection lorsqu'ils se trouvent au bureau ou qu'ils se déplacent ailleurs.
- L'équipement portatif et les supports contenant des renseignements judiciaires devraient être placés en lieu sûr derrière des portes verrouillées.

- L'équipement devrait être étiqueté en permanence d'une façon évidente qui facilite l'identification ou, si l'EMR le recommande, comporter également des vignettes d'identification discrètes. Il y a lieu de procéder à des vérifications régulières afin de s'assurer que l'équipement se trouve à l'endroit qui lui a été désigné.

- Lorsqu'un utilisateur judiciaire n'a plus besoin d'accéder aux renseignements judiciaires, toutes les clés doivent être récupérées, les cartes d'accès doivent être retournées et désactivées et les codes d'accès doivent être modifiés. Tous les codes d'accès des utilisateurs devraient être modifiés périodiquement dans tous les cas (au moins une fois l'an).

7. Classification des renseignements judiciaires

Politique 7 : Les cours devraient adopter un système de classification permettant l'identification des renseignements judiciaires sensibles afin de leur assurer une protection spéciale. Les renseignements classifiés doivent être divulgués uniquement aux personnes qui ont besoin de les connaître.[17]

Commentaires

101. Les cours devraient établir un système de classification à l'égard des renseignements judiciaires. Les documents classifiés doivent faire l'objet d'un traitement spécial tout au long de leur cycle de vie, de façon que seuls les utilisateurs ayant l'autorisation nécessaire puissent y avoir accès.[18]

102. L'auteur d'un document devrait être responsable d'attribuer la classification qui convient aux renseignements qu'il a créés.

103. L'accès aux renseignements classifiés est contrôlé dans le cadre de la gestion du système ainsi que des mesures de contrôle d'accès techniques et opérationnelles (voir la politique 8). Seules les personnes ayant légitimement besoin de connaître les renseignements classifiés devraient obtenir l'accès à ceux-ci pour les lire ou les modifier (selon le cas). L'auteur détermine les personnes ayant besoin de connaître les renseignements.

Classification

104. Le système de classification à deux paliers qui suit constitue un modèle très simple que les cours pourraient utiliser. Il pourrait également être possible d'adopter les systèmes de classification des gouvernements fédéral et provinciaux.

> ***Renseignements réservés aux utilisateurs judiciaires*** – Tous les renseignements judiciaires sont classifiés par défaut « réservés aux utilisateurs judiciaires » et par le fait même sont assujettis aux mesures de protection décrites dans le Plan d'action.

---

17 Un système de classification des renseignements n'est efficace que s'il est lié à une procédure de filtrage du personnel qui est conçue pour garantir que ceux qui ont accès à des renseignements classifiés sont fiables. Voir Wood, section 6, qui propose diverses politiques concernant les questions de ressources humaines.

18 Dans le cadre de leur travail, les juges manient déjà des renseignements qui sont susceptibles de recevoir un traitement spécial, telles les ordonnances de non-publication ou les interdictions réglementaires. Le Plan d'action ne suggère pas d'outrepasser les autres systèmes de classification qui sont susceptibles de s'appliquer dans le contexte judiciaire. Voir aussi Wood, section 5.02, et la norme ISO 17799, section 7.2.

Renseignements protégés – Cette classification peut être utilisée pour des renseignements judiciaires très sensibles, par exemple : des documents qui contiennent des renseignements personnels qui peuvent concerner les juges ou encore des litiges ou des parties, des projets de jugement, les courriels liés à un avis judiciaire et à la jurisprudence ainsi que les notes et mémoires portant sur des questions qui concernent la magistrature. Les renseignements protégés seraient sujets à un traitement plus rigoureux qui inclurait un étiquetage particulier, le chiffrement et l'entreposage sur des supports désignés.

105. L'auteur est responsable de décider quand les renseignements judiciaires ne sont plus classifiés et peuvent être divulgués à des utilisateurs non judiciaires. Par exemple, lorsque l'ébauche d'un jugement est finalisée, elle peut être rendue publique conformément aux instructions du juge.

Métadonnées

106. Les juges doivent être conscients que certains fichiers informatiques – par exemple les projets de jugement – peuvent contenir du texte supprimé, l'historique des révisions d'un texte, ainsi que des renseignements personnels incorporés qui, même s'ils sont cachés, sont faciles à récupérer. Ces données incorporées sont communément appelées « métadonnées ». Afin d'éviter que les destinataires de fichiers électroniques – par exemple les fichiers joints à un courriel – puissent obtenir accès à de quelconques renseignements de nature délicate, les utilisateurs judiciaires devraient s'assurer que tous les fichiers informatiques qui quittent l'environnement sécurisé des cours soient libres de métadonnées. L'élimination des métadonnées est une fonction administrative qui doit être effectuée au moyen d'outils logiciels appropriés. Les logiciels et les procédures servant à l'élimination des métadonnées devraient être vérifiés et validés par l'agent de la sécurité informatique du système judiciaire.

Mise en oeuvre

107. Voici quelques-unes des caractéristiques clés d'un système de classification efficace :

- Tous les utilisateurs doivent connaître le système de classification.
- Lorsqu'un système, une compilation (base de données) ou un support de données renferme des renseignements classifiés, tout le système, la base de données ou le support doit être ainsi classifié.
- La classification s'applique aux renseignements à compter du moment où ceux-ci sont reçus ou créés jusqu'à celui où ils sont détruits ou déclassifiés.

- Tous les renseignements classifiés doivent comporter une mention, par étiquette ou autrement, de la désignation qui s'applique à eux. Ainsi, un filigrane, un en-tête ou un pied de page doit figurer sur chaque page des documents électroniques. Pour les courriels, une signature désignant le niveau de classification peut être utilisée. Les systèmes employés devraient être uniformes et comporter un modèle de structure pour les applications.

- Lorsque des renseignements électroniques classifiés sont stockés sur des disques ou des bandes, imprimés sur copie papier ou télécopiés depuis l'ordinateur, tous les supports doivent être étiquetés de façon convenable et la désignation de la classification doit figurer de façon bien visible sur toutes les copies papier, les pages de titre et les feuilles d'envoi.

- Les renseignements classifiés ne doivent pas être imprimés au moyen d'une imprimante non surveillée.

- Lorsque les renseignements classifiés sont stockés sur des supports amovibles ou de l'équipement portatif, ils doivent être surveillés personnellement ou rangés dans un endroit verrouillé en tout temps.

- Lorsque des bandes de sauvegarde sont entreposées à l'extérieur des lieux, les renseignements classifiés doivent être sauvegardés sous forme codée (voir également la politique 5).

108. Il existe de nombreuses autres mesures de contrôle que les cours devraient songer à appliquer à l'égard des renseignements classifiés. Le lecteur trouvera un bon exemple de politique concernant la classification des données dans Wood, section 5.02.01.

Section 3 : Mesures de protection techniques

109. La gestion des systèmes modernes comprend la capacité de concevoir et de configurer les réseaux, le matériel et le logiciel de façon à appuyer les politiques en matière de sécurité informatique et à rehausser (et même automatiser) les mesures de protection opérationnelles. La présente section du Plan d’action traite des mesures de contrôle d’accès au système, des mesures de contrôle de l’accès à distance, du chiffrement, des pare-feux, des systèmes de détection d’intrusion et de la protection antivirus.

8. Contrôle de l'accès aux systèmes des cours

Politique 8 : Les cours doivent mettre en oeuvre des mesures de contrôle d'accès strictes afin que seuls les utilisateurs autorisés aient accès aux systèmes judiciaires et que leur niveau d'accès corresponde à l'autorisation d'accès qu'ils ont obtenue ainsi qu'au système de classification des renseignements de la cour concernée. Il appartient aux juges de déterminer les droits d'accès aux

Commentaires

110. Les systèmes des cours devraient comporter des mécanismes d'authentification des personnes qui sont autorisées à les utiliser. (Voir Wood, section 9.0, pour un ensemble détaillé de politiques concernant le contrôle de l'accès. Voir aussi la norme ISO 17799, section 11, « Access Control ».)

111. Une simple combinaison d'un nom d'utilisateur unique (ou « nom de connexion ») ainsi que d'un mot de passe offre une certaine sécurité minimale. Cependant, les mots de passe peuvent être communiqués, volés, devinés ou calculés. Pour que l'authentification soit plus sûre, il y a lieu d'utiliser une combinaison de méthodes et de technologies plus élaborées comme des mots de passe dynamiques, des cartes à puce, des jetons USB, des certificats de clé publique et des procédés biométriques.

112. L'accès logique aux renseignements judiciaires devrait être consigné et vérifié systématiquement par l'agent de la sécurité informatique du système judiciaire. L'accès aux renseignements judiciaires devrait se faire seulement par la voie de personnes désignées et l'usage de comptes administratifs génériques devrait être évité. Les personnes qui ont des privilèges administratifs devraient avoir un compte administratif qui est distinct de leur compte d'utilisateur personnel.

113. L'emploi de mots de passe dynamiques, qui sont générés par de petits dispositifs portatifs comme des jetons, a pour effet de modifier le mot de passe de l'utilisateur chaque fois que celui-ci ouvre une session. En l'absence d'un mot de passe produit par jeton, la connexion est très difficile, voire impossible. Utilisés en combinaison avec un mot de passe statique, ces dispositifs empêchent qui que ce soit de deviner ou de voler le mot de passe d'une autre personne.

114. D'autres moyens de contrôle comme les cartes à puce reposent sur l'utilisation de certificats de clé publique, qui constituent une forme d'identification codée de l'utilisateur. Pour sa part, la biométrie est fondée sur l'utilisation des caractéristiques physiques de l'utilisateur, comme la reconnaissance d'empreintes digitales ou d'empreintes rétiniennes. Toutes les mesures de contrôle de l'accès présentent des inconvénients aux utilisateurs. Les cours doivent s'efforcer d'encourager tous les utilisateurs à ne pas contourner ni éluder ces mesures.

115. Chaque cour devrait établir des protocoles relatifs aux autorisations de sécurité de façon que, lorsque les utilisateurs ouvrent une session et sont reconnus, leurs droits d'accès soient limités à un niveau correspondant à leur tâche. Ainsi, les administrateurs du système ont habituellement plus de droits que les utilisateurs. Les droits habituels comprennent l'accès à certains serveurs, dossiers, applications, caractéristiques ou fonctions. (Une bonne partie des questions qu'il importe d'examiner à cet égard sont traitées au chapitre 10 du Manuel du CST.)

Accès aux renseignements judiciaires classifiés

116. Seuls les juges devraient prendre les décisions concernant les droits d'accès aux renseignements judiciaires classifiés. Voici quelques-unes des décisions qui doivent être prises :

- les décisions qui concernent l'accès aux applications, aux caractéristiques ou à la fonctionnalité du système et qui pourraient avoir des répercussions sur les renseignements judiciaires classifiés;
- les décisions concernant la disponibilité de l'accès à distance ou de l'accès aux systèmes dans plusieurs palais de justice;
- les décisions concernant un système donné de classification des renseignements (voir la politique 7);
- les décisions concernant la façon dont l'accès est supprimé et les fichiers (ainsi que les bandes de sauvegarde) sont archivés ou supprimés ainsi que les moments où ces mesures sont prises;
- les décisions concernant l'espace du disque serveur attribué aux juges;
- toute décision ou politique concernant la surveillance possible des utilisateurs judiciaires.

Protocoles générateurs de mots de passe

117. Les administrateurs de système devraient veiller à ce que les utilisateurs se conforment aux pratiques exemplaires en ce qui a trait à l'usage de leur mot de passe. Le document intitulé « La protection en dix points des renseignements judiciaires informatisés », qui figure à l'annexe 4, offre quelques exemples.

118. Le système de la cour devrait exécuter régulièrement des modifications de mots de passe et configurer tous les ordinateurs portatifs à l'aide de mots de passe mis sous tension.

119. La sécurité des produits des travaux et des autres renseignements des juges qui partagent des systèmes de messagerie intra-entreprise pourrait être compromise si les juges sont inscrits comme des utilisateurs d’une façon qui ne les différencie pas des autres utilisateurs. Ainsi, lorsque les noms d’utilisateur jwatson@court.ca et jane_watson@court.ca correspondent respectivement à un juge et à un procureur de la Couronne inscrits dans le système, il y a plus de chances que des messages soient envoyés par inadvertance au mauvais destinataire.

9. Contrôle de l'accès à distance et réseaux sans fil

Politique 9 : Des mesures spéciales doivent être prises pour assurer la sécurité et la confidentialité de toutes les connexions à distance et de la réseautique sans fil.

Commentaires[19]

120. Les juges canadiens se déplacent fréquemment et bon nombre d'entre eux présument qu'ils peuvent facilement avoir accès à distance aux systèmes de renseignements judiciaires. En plus de tenir compte des problèmes et enjeux plus généraux qui sont liés au contrôle de l'accès et qui sont commentés plus haut dans la section portant sur les systèmes de contrôle d'accès, il y a lieu de mettre en oeuvre des mesures de contrôle axées explicitement sur la sécurité de l'accès à distance et l'utilisation d'appareils portatifs. Lorsque l'accès à distance au réseau interne est autorisé, la cour devient vulnérable face aux pirates informatiques et à d'autres intrus qui seraient tentés d'explorer et d'attaquer les systèmes de réseau. Étant donné que l'accès à distance et l'utilisation d'appareils portatifs comportent des risques spéciaux, les cours doivent adopter des mesures de contrôle précises à cet égard.

121. En raison de risques liés au fait de permettre l'accès au réseau interne, il est crucial de savoir exactement qui sont les utilisateurs à distance, quels sont les besoins et comment intégrer des mesures de contrôle de l'accès à distance dans un plan de sécurité. La nécessité d'un accès à distance protégé (ADP) ne se fait pas sentir uniquement du côté des utilisateurs judiciaires.

122. Lorsque les utilisateurs entrent en communication avec le système judiciaire à l'aide d'un modem ou d'une ligne téléphonique ordinaire, les cours devraient envisager l'adoption des lignes directrices suivantes en ce qui a trait à la connexion à des services centralisés de modem ou à un serveur d'accès à distance (SAD) au palais de justice :

> **Identification de l'appelant** - le serveur d'accès à distance vérifie le numéro de téléphone d'un appelant par rapport à une liste approuvée de numéros de téléphone. Si les numéros de téléphone correspondent, l'utilisateur obtient accès au réseau. (Cette méthode ne touche pas les utilisateurs mobiles.)

[19] Wood donne des exemples de politiques relatives à la sécurité du télétravail et des ordinateurs mobiles à la section 9.08 de son ouvrage. Voir aussi la norme ISO 17799, section 11.7.

Systèmes de sécurité par rappel automatique - lorsqu'un utilisateur entre en contact avec le réseau, le modem de réponse demande l'identification de l'appelant, interrompt la communication, vérifie l'identification de l'appelant par rapport à un annuaire et rappelle ensuite le modem autorisé au numéro correspondant à l'identification de l'appelant, ce qui empêche l'accès aux pirates éventuels. Cette façon de procéder permet de veiller à ce que les données soient communiquées uniquement entre des dispositifs autorisés. Même si les techniques de rappel fonctionnent bien pour l'accès de type branchement et les entrées en communication depuis le domicile de l'utilisateur, la plupart des produits de connexion par rappel ne conviennent pas aux utilisateurs mobiles, qui changent souvent d'endroit de jour en jour. Il existe maintenant des produits qui acceptent des numéros de rappel mobiles, ce qui permet à ces utilisateurs d'appeler un serveur d'accès à distance ou un ordinateur hôte, d'entrer leur code d'utilisateur et leur mot de passe, puis de préciser un numéro où le serveur ou l'ordinateur les rappellera[20]. Le numéro de rappel est ensuite consigné et il sera possible d'utiliser ce renseignement plus tard pour déceler les failles en matière de sécurité.

123. L'authentification des utilisateurs à distance devrait être nécessaire afin que seuls les membres autorisés du personnel aient accès au réseau de la cour.

124. Lorsque les utilisateurs ont accès au système de la cour à l'aide d'un dispositif de connexion à haute vitesse numérique obtenu d'un fournisseur de service Internet (FSI) haute vitesse par câble ou par téléphone, il y aurait lieu de fournir aux juges des logiciels de pare-feu ainsi que des dispositifs permettant la création de VPN (réseaux privés virtuels) par chiffrement[21].

Réseaux sans fil

125. Les réseaux sans fil offrent aux utilisateurs beaucoup de commodité et de mobilité, mais ils sont moins sûrs que les systèmes câblés. Les cours doivent veiller à ce que tous les utilisateurs judiciaires de réseaux sans fil, tant à l'intérieur qu'à l'extérieur des palais de justice, soient suffisamment protégés contre les risques de sécurité, en offrant aux utilisateurs une formation efficace et en utilisant des pare-feux individuels, entre autres mesures. Voir Wood, sections 8.05.01 et 53 à 59.

---

[20] Cette situation pourrait poser des problèmes dans les endroits comme les chambres d'hôtel où les juges logent pendant leurs déplacements et qui n'offrent pas d'installations de connexion téléphonique analogique.

[21] [TRADUCTION] « VPN est l'acronyme de *virtual private network* (réseau privé virtuel), c'est-à-dire un réseau qui est construit par l'utilisation d'un réseau public pour relier des ordinateurs nodaux. Ainsi, il existe certains systèmes qui permettent de créer des réseaux en utilisant Internet pour le transport des données. Ces systèmes se fondent sur le chiffrement et d'autres mécanismes de sécurité pour limiter l'accès au réseau aux utilisateurs autorisés et empêcher l'interception des données ». Voir Webopedia, http://www.webopedia.com/TERM/V/VPN.html .

126. Les réseaux locaux sans fil et les dispositifs de connexion d'appareils sans fil (comme Bluetooth[22]) doivent être configurés, protégés et testés convenablement et ils doivent être pleinement conformes à tous les aspects de la politique de sécurité des renseignements, notamment :

    - adopter la nouvelle norme WPA2 (aussi appelée IEEE 802.11i) pour tous les réseaux sans fil, étant donné que le WEP (Wired Equivalent Privacy) est peu sûr;[23]
    - ne pas diffuser les identificateurs de service;
    - changer l'identificateur de service implicite et les mots de passe des routeurs;
    - désactiver les fonctions de gestion à distance.

Appareils portatifs

127. Un nombre grandissant de juges utilisent des appareils portatifs comme les téléphones intelligents, les assitants numériques personnels (PDA), les appareils « Blackberry » et d'autres appareils portatifs. Tous les appareils de ce genre devraient être configurés de manière à être protégés convenablement avant d'être distribués, et tous les utilisateurs doivent recevoir une formation pour apprendre à s'en servir efficacement.

Voix sur IP (Voix sur protocole Internet)

128. Voix sur IP est une technologie qui achemine les communications téléphoniques par la voie de réseaux comme Internet au lieu du traditionnel réseau téléphonique commuté public. Bien que cette technologie permette de réaliser des économies et qu'elle offre de nombreuses caractéristiques avantageuses, comme l'intégration des messageries de bureau, elle comporte aussi des risques de sécurité. Si les cours font usage de Voix sur IP, elles doivent veiller à ce que le système soit doté du niveau de sécurité le plus élevé. Voir Wood, sections 8.07.07 et 28 à 31.

---

[22] Pour plus de renseignements sur la sécurité de Bluetooth, voir http://ww.bluetooth.com/Bluetooth/Learn/Security.

[23] Pour des renseignements techniques à ce sujet, voir Dan Thompson, « Implementing a Secure Wireless Network for a Windows Environment », SANS Institute, http://www.sans.org/reading_room/whitepapers/wireless/1619.php .

10. Indépendance judiciaire

Politique 10 : La configuration des systèmes de contrôle d'accès des cours doit être conforme au principe de l'indépendance judiciaire. Les utilisateurs judiciaires devraient disposer d'un accès exclusif à leurs propres ressources réseau, à moins qu'il ne puisse être démontré que l'architecture, la configuration, les mécanismes de contrôle d'accès, le soutien opérationnel et les systèmes de classification des renseignements du réseau concerné soient suffisants pour assurer une confiance absolue dans la séparation des renseignements judiciaires et non judiciaires et pour assurer la conformité au Plan d'action et aux Lignes de conduite sur la surveillance informatique du Conseil.

Commentaires

129. Les réseaux informatiques modernes sont similaires à des couloirs ou à des canalisations de communication partagés par de nombreuses personnes, dont des résidents et des visiteurs. Bien que le réseau en soi puisse être accessible à des utilisateurs qui détiennent des cotes de sécurité variées, seuls ceux qui sont autorisés ont accès à des pièces spécifiques sécurisées. Munis des mesures de sécurité appropriées, les utilisateurs judiciaires de même que les renseignements judiciaires peuvent être compartimentés efficacement et protégés à même un seul réseau partagé. (Voir Wood, section 9.04.06, et la norme ISO 17799, section 11, « Access Control ».)

130. Certains membres du Conseil sont préoccupés par la gestion de la sécurité sur des serveurs partagés dans leurs juridictions. Ils croient que les renseignements judiciaires ne sont pas suffisamment protégés par des mesures de sécurité administratives appropriées et que la seule façon de protéger totalement ces renseignements consisterait à recourir, pour les utilisateurs judiciaires, à un réseau physique totalement séparé.

131. Le Conseil est également préoccupé par le principe de l'indépendance judiciaire. L'entreposage en commun de renseignements judiciaires et non judiciaires, de même que la présence des procureurs de la Couronne et de policiers comme utilisateurs du même réseau à titre d'utilisateurs judiciaires, peut avoir l'apparence de compromettre cette indépendance.

132. Ces préoccupations sont telles que certains juges n'enregistrent le fruit de leur travail que sur des disquettes amovibles ou sur leur lecteur de disque dur local plutôt que sur les lecteurs du réseau fournis par la cour.

133. La création ou l'utilisation d'un réseau physique séparé pour les utilisateurs judiciaires permettrait non seulement de régler le problème de l'indépendance des juges, mais offrirait aussi plusieurs autres avantages, notamment :

- une application plus facile des mesures de contrôle d'accès et du système de classification;
- la conformité avec les Lignes de conduite sur la surveillance informatique;
- des moyens plus efficaces de faire en sorte que les copies de sauvegarde contiennent uniquement des renseignements judiciaires.

134. Toutefois, il peut aussi y avoir des obstacles pratiques et économiques à la création ou à l'utilisation d'un réseau physique distinct à l'intention des utilisateurs judiciaires, notamment :

- des obstacles techniques pour les utilisateurs judiciaires qui doivent avoir accès aux systèmes de gestion des instances et aux autres systèmes d'administration des cours; la limitation touchant l'accès à des renseignements qui pourraient être utiles pour l'ensemble du système judiciaire;
- l'ajout de frais importants découlant de la création, de la gestion et du soutien de réseaux informatiques parallèles;
- des inconvénients supplémentaires pour les utilisateurs judiciaires qui auraient à accéder à au moins deux systèmes réseaux.
- de petits réseaux réservés aux juges pourraient être encore plus exposés à un risque d'atteinte à la sécurité que des réseaux plus gros et plus sophistiqués.

11. Chiffrement

Politique 11 : Les cours doivent mettre à la disposition des utilisateurs judiciaires une technologie de chiffrement à jour pour le stockage et la transmission des renseignements judiciaires classifiés sur les réseaux, les ordinateurs de bureau et les ordinateurs portatifs.

Commentaires

135. Les logiciels, les normes et les protocoles de gestion qui servent à chiffrer les données à l'aide de certificats numériques constituent ce qu'on appelle l'infrastructure à clé publique.

136. Le certificat numérique, attribué par une tierce partie de confiance, vérifie l'identité de l'utilisateur et relie ce dernier à une clé publique unique, ce qui permet d'échanger et de déchiffrer les messages chiffrés. Afin d'assurer une indépendance complète, il est recommandé que l'autorité de certification des utilisateurs judiciaires soit une tierce partie de confiance indépendante non seulement de la magistrature mais aussi du gouvernement.

137. Les renseignements judiciaires qui sont classifiés devraient être chiffrés avant d'être transmis sur un réseau public. Cependant, si les techniques de chiffrement ne sont pas administrées convenablement, cela pourrait compromettre la capacité de la cour de vérifier les systèmes informatiques internes.

138. La décision de chiffrer des données devrait être fondée sur des évaluations gestionnelles documentées des risques liés à la sécurité ainsi que sur l'application du système de classification des renseignements judiciaires.

- Toute personne qui utilise une technique de chiffrement des renseignements judiciaires doit être connue de l'agent de la sécurité informatique du système judiciaire et fournir des renseignements concernant la fonctionnalité du produit.

- L'agent de la sécurité informatique du système judiciaire devrait donner des directives à tous les utilisateurs au sujet de l'emploi de la technologie du chiffrement et élaborer et consigner par écrit des procédures relatives au recouvrement des renseignements chiffrés. L'agent de la sécurité informatique du système judiciaire devrait également surveiller toutes les demandes de certificats que soumettent les utilisateurs[24].

[24] Le certificat est un document numérique qui sert à authentifier les utilisateurs et à sécuriser la transmission de renseignements sur des réseaux publics.

12. Pare-feux

Politique 12 : Tous les réseaux des cours où se trouvent des renseignements judiciaires doivent être protégés des réseaux extérieurs, y compris Internet, au moyen d'une technologie de pare-feu appropriée qui est administrée de manière efficace. Toutes les connexions depuis un réseau de la cour à des réseaux extérieurs doivent passer par des pare-feux approuvés.

Commentaires[25]

139. Les pare-feux constituent un élément important d'un réseau protégé.[26] Ils offrent une passerelle de sécurité vers d'autres réseaux et protègent la confidentialité, l'intégrité et la disponibilité des renseignements judiciaires. Les pare-feux peuvent être configurés de façon a) à empêcher le trafic non désiré sur le réseau et b) à dissimuler de l'Internet des renseignements comme les noms de système, la topologie de réseau, les types de dispositifs réseaux et les identificateurs d'utilisateurs internes.

140. Pour assurer l'efficacité des systèmes pare-feu, il est nécessaire de mener des activités de recherche et de planification considérables et de comprendre à fond les activités, le réseau, l'architecture des systèmes ainsi que les politiques en matière de sécurité de la cour. Le Plan d'action fournit des lignes directrices générales de base concernant l'obtention, l'installation, la configuration et la maintenance d'un pare-feu réseau.

141. Les pare-feux ne constituent pas une garantie absolue de la sécurité du réseau et, en fait, ils peuvent donner une illusion de sécurité à certains utilisateurs. Ils offrent simplement une défense périmétrique autour d'un réseau. Dès qu'un pirate (qui peut être un utilisateur autorisé) obtient l'accès au réseau protégé, tous les systèmes sont en danger.

142. De plus, les pare-feux n'empêchent pas les attaques pouvant se produire par l'entremise de « portes dissimulées » du réseau, comme les liaisons commutées par modem, les liaisons directes par ligne louée ou d'autres points de départ du réseau. Seul le trafic réseau qui passe par le pare-feu sera conforme aux règles de celui-ci; le pare-feu ne peut appliquer une politique à l'encontre du trafic qui passe par d'autres points d'entrée du réseau.[27]

---

[25] Wood donne des exemples de politiques sur les pare-feux au chapitre 20, p. 633, et aux sections 8.05.01 et 21 à 27. Voir également les sections 31 à 33.

[26] Le SANS Institute propose plusieurs articles utiles sur les pare-feux à http://rr.sans.org/.

[27] Il faut également tenir compte d'autres types de trafic malveillant, tels les chevaux de Troie ou des programmes clés d'ouverture de session, puisqu'aucun pare-feu n'est en mesure de tout bloquer.

143. Lorsque le réseau d'une cour comporte une connexion Internet spécialisée, un pare-feu commercial autonome doit être en place afin de protéger le réseau. Il est également souhaitable de veiller à ce que les serveurs d'applications et de fichiers ne fonctionnent pas également comme serveurs de communication.

144. Les communications d'arrivée dans les systèmes des cours doivent passer par un système d'identification et d'autorisation d'accès.

145. Lorsque l'ordinateur de bureau ou l'ordinateur portatif d'une cour est relié à Internet au moyen d'une ligne commutée ou d'une connexion spécialisée, un pare-feu personnel devrait être installé et configuré de façon satisfaisante sur cet ordinateur.

146. En général, le pare-feu devrait comporter les caractéristiques et capacités suivantes :

- le pare-feu est un produit d'un vendeur établi dont les produits ont été certifiés par les autorités gouvernementales;[28]
- le pare-feu est accrédité par un organisme de normalisation national ou international;
- le pare-feu appuie une politique fondée sur le refus de tous les services, sauf ceux qui sont explicitement autorisés, même s'il ne s'agit pas de la politique appliquée à l'origine;
- le pare-feu appuie une politique en matière de sécurité adaptée au système de la cour;
- le pare-feu peut être adapté aux nouveaux besoins et services lorsque la politique en matière de sécurité de l'organisation est modifiée;
- le pare-feu comporte des mesures d'authentification avancées ou appuie la capacité d'installer des mesures de cette nature;
- le pare-feu repose sur l'emploi de techniques permettant ou refusant des services à certains systèmes hôtes, au besoin;
- le pare-feu consigne l'accès à la passerelle et par l'entremise de celle-ci;

---

[28] Au Canada, une liste nationale de pare-feux et de RPV qui ont été présélectionnés par le CST se trouve à l'adresse : http://www.cse-cst.gc.ca/services/industrial-services/its-pre-qual-prod-list-f.html.

- le pare-feu repose sur l'emploi d'un dispositif de filtrage souple et convivial qu'il est facile de programmer et qui peut filtrer un large éventail d'attributs, y compris l'adresse IP source et destination, le type de protocole, le port TCP/UDP source-destination et l'interface entrée-sortie;

- lorsque le pare-feu nécessite un système d'exploitation, comme le système UNIX, une version protégée du système devrait être incluse ainsi que les autres dispositifs de sécurité qui sont nécessaires pour assurer l'intégrité de l'ordinateur hôte du pare-feu; de plus, tous les correctifs du système d'exploitation devraient être installés;

- la puissance et la précision du pare-feu doivent être vérifiables. La conception du pare-feu doit être simple, afin que les administrateurs puissent le comprendre et en assurer la maintenance. Le pare-feu et le système d'exploitation correspondant devraient être mis à jour au moyen des correctifs et autres corrections de bogues;

- les services de soutien technique devraient être inclus;

- des services de formation devraient être inclus;

- la documentation relative au système devrait être incluse.

13. Système de détection d'intrusion

Politique 13 : Les cours doivent établir une procédure d'ouverture de session sur tous les serveurs et dispositifs du réseau afin de détecter les tentatives d'accès non autorisé et les séquences d'opérations suspectes. Toute activité de ce type de la part des utilisateurs judiciaires est assujettie en tout temps aux Lignes de conduite sur la surveillance informatique et doit être portée à l'attention de l'agent de la sécurité informatique du système judiciaire. Dans les cas où l'EMR le recommande, les cours devraient installer des systèmes de détection d'intrusion en versions réseau et intégrée assurant un signalement automatique des intrusions en temps réel.

Commentaires[29]

147. La détection d'intrusion consiste à surveiller l'activité d'un système ou réseau informatique et à l'analyser pour y déceler des signes d'intrusion. L'intrusion est définie comme une tentative visant à compromettre la sécurité d'un ordinateur ou d'un réseau. Il est possible de détecter les intrusions, soit en examinant manuellement les registres générés par le système et en prenant les mesures qui s'imposent, soit en utilisant un logiciel qui permet d'examiner et d'analyser automatiquement les traces d'intrusion et d'intervenir. L'utilisation combinée des approches manuelle et automatique est généralement appropriée.

148. Le logiciel du système de détection d'intrusion (SDI) surveille les systèmes informatiques et le trafic réseau et analyse ces données pour y déceler les attaques hostiles provenant de l'extérieur de la cour ainsi que les usages malveillants et les attaques émanant de l'intérieur. Le principal avantage d'un SDI réside dans le fait qu'il offre une image plus claire de l'activité sur le serveur et le réseau et transmet des signaux d'avertissement afin de prévenir les administrateurs du système d'une activité non autorisée ou inhabituelle.

149. Étant donné que la détection des intrusions nécessite forcément la surveillance des systèmes, tous les systèmes de détection d'intrusion qu'une cour utilise doivent être conformes aux Lignes de conduite sur la surveillance informatique (voir l'annexe 2), selon laquelle a) les renseignements que les utilisateurs judiciaires conservent sur leur ordinateur ne peuvent faire l'objet de surveillance et b) dans la mesure où la surveillance des utilisateurs judiciaires est nécessaire à des fins de sécurité, elle devrait être faite par ceux-ci, sous la direction de l'agent de la sécurité informatique du système judiciaire.

150. La magistrature doit élaborer des lignes directrices claires et détaillées à l'égard de l'administration des système afin de réduire les risques de conflit.

---

[29] Voir Wood, section 9.07, et sections 8.05.01, 19, 20, 8.01.03, 5 et 6.

Types de systèmes de détection d'intrusion

151. À l'heure actuelle, deux grands types de systèmes de détection d'intrusion sont disponibles : la version réseau et la version hôte. Certains vendeurs offrent l'un ou l'autre de ces types de produit; cependant, la solution intégrée, qui réunit les deux types de systèmes, est de plus en plus populaire : grâce à la gestion centralisée dont il fait l'objet, ce système permet d'accroître la résistance du réseau aux intrusions ainsi que la souplesse au plan de la mise en place des produits.

152. Version hôte - Lorsque la détection des intrusions se fait au niveau de l'hôte, le logiciel réside sur un serveur et surveille les registres de celui-ci (ainsi que certaines applications) afin d'y déceler les tentatives d'accès non autorisé et les comportements aberrants. L'agent de la sécurité informatique du système judiciaire devrait rédiger les règles de la détection au niveau de l'hôte qui déclenchent l'analyse des listes de contrôle et registres d'événements. Le système peut ensuite évaluer cette action, comme les activités des utilisateurs ou d'ouverture de session ou encore les activités entourant les comptes ou les applications de ceux-ci. Cette analyse permet de déceler les comportements aberrants d'utilisateurs locaux ou éloignés qui peuvent indiquer des tentatives d'accès non autorisé au système.

153. Version réseau - Ce type de SDI est un senseur qui réside sur un serveur de réseau local. Il filtre et analyse les transmissions de données sur le réseau en temps réel et les compare à une base de données des comportements ou signatures d'attaque connus. Les signatures d'attaque sont des moyens connus que les intrus ont utilisés dans le passé pour pénétrer un réseau.

154. Les facteurs suivants devraient être pris en compte lors de la sélection des systèmes de détection d'intrusion :

- le vendeur doit être bien établi et ses produits doivent être certifiés par le gouvernement;
- le système devrait être accrédité par un organisme de normalisation national ou international;
- le SDI devrait pouvoir fonctionner en même temps que les activités de gestion de réseau;
- le SDI doit pouvoir s'adapter à l'évolution des besoins de la cour en matière de sécurité;

- le système devrait couvrir les mises à jour des abonnements et des signatures;
- de la documentation ainsi que des services de formation et de soutien techniques devraient être fournis.

Administration

155. Tous les registres de vérification du système devraient être examinés tous les jours, conformément aux Lignes de conduite sur la surveillance informatique.

156. Les utilisateurs devraient recevoir la formation voulue pour signaler toute anomalie du système. L'agent de la sécurité informatique du système judiciaire devrait surveiller l'examen de tous les rapports de dérangement et les signes d'intrusion qu'ils comportent.

157. Il y a lieu de vérifier régulièrement les SDI au niveau de l'hôte afin de s'assurer qu'ils donnent le rendement voulu.

158. L'agent de la sécurité informatique du système judiciaire devrait tenir des fichiers de signature du SDI (fichiers servant à déceler les intrusions possibles d'après les caractéristiques du trafic réseau) actualisés et en assurer la mise à jour en temps opportun.

159. L'agent de la sécurité informatique du système judiciaire devrait établir des liens avec des organismes spécialisés en intervention en cas d'incident informatique ainsi qu'avec ses homologues des autres cours et échanger des renseignements concernant les menaces, vulnérabilités et incidents pertinents découverts.

14. Protection contre les codes malveillants, le pourriel et les menaces connexes

Politique 14 : Tous les systèmes des cours doivent employer des logiciels conformes aux normes de l'industrie pour assurer la détection en temps réel des codes malveillants, du pourriel et des menaces connexes et pour assurer une protection contre ceux-ci.

Politique 15 : Dans toute la mesure du possible, de tels systèmes de protection doivent être installés sur les pare-feux, les serveurs, les postes de travail locaux, les ordinateurs portatifs, les appareils portatifs et les ordinateurs domestiques qui renferment des renseignements judiciaires ou qui servent à accéder à de tels renseignements.

Politique 16 : Tous les utilisateurs doivent recevoir une formation sur les pratiques exemplaires à suivre pour réduire les risques de codes malveillants, de pourriel et de menaces connexes.

Commentaires[30]

160. Depuis l'arrivée du courrier électronique et l'utilisation répandue du Web, les codes malveillants sont devenus une menace majeure pour la sécurité. Il est facile de transmettre des virus et des vers dans le monde entier en peu de temps en joignant aux messages électroniques des fichiers exécutables infectés. Les pièces jointes sont habituellement des « chevaux de Troie » qui sont présentés comme un objet que le destinataire a demandé ou qu'il aimerait voir et qui semblent souvent provenir d'une source connue. Les logiciels publicitaires et les logiciels-espion sont des types apparentés de codes malveillants. Ils sont souvent enfouis dans des logiciels gratuits qui paraissent légitimes, de telle sorte que lorsqu'un utilisateur télécharge un tel logiciel, le logiciel-espion s'installe subrepticement en même temps. Généralement, les codes malveillants prennent le contrôle des ordinateurs ciblés et ils s'en servent pour lancer d'autres attaques coordonnées sur les sites Web de tiers ou pour obtenir accès à des renseignements personnels comme des mots de passe.

[30] Voir Wood, section 8.03.01, et la norme ISO 17799, section 10.4.

161. Selon certaines estimations, le pourriel, c'est-à-dire du courriel non sollicité et envoyé massivement, représente aujourd'hui de 75 % à 85 % de tout le courrier électronique circulant dans le monde.[31] En plus d'être un irritant, le pourriel sert également à tromper les destinataires et à les amener par la ruse à révéler des renseignements personnels au moyen d'une technique d'ingénierie sociale appelée « l'hameçonnage ».[32]

162. La meilleure défense contre les codes malveillants consiste à appliquer des pratiques de gestion efficaces, conjuguée à l'utilisation de logiciels de protection installés sur les pare-feux, les serveurs, les postes de travail, les ordinateurs portatifs et les appareils portatifs. Un logiciel de protection complet devrait comprendre les éléments suivants : un filtre de pourriel programmable; un programme de détection qui vérifie les fichiers et les répertoires électroniques afin d'y déceler la présence de codes malveillants; un « désinfectant » qui élimine les codes malveillants des fichiers infectés; une protection en temps réel contre le pourriel et les codes malveillants; et un service d'abonnement aux mises à jour automatiques qui permet à l'utilisateur de continuer à bénéficier de la protection au fur et à mesure que de nouvelles menaces sont découvertes.

163. Les facteurs suivants devraient être pris en compte dans la sélection d'un logiciel de filtrage du pourriel et de détection de codes malveillants :

- le vendeur devrait être bien établi et, si possible, ses produits devraient être certifiés par les autorités gouvernementales;[33]
- le système devrait être accrédité par un organisme de normalisation national ou international;
- le logiciel devrait comporter à la fois un moteur de balayage servant à détecter les menaces connues et un moteur heuristique permettant de déceler les macro-virus;
- le vendeur devrait fournir des mises à jour automatiques des fichiers de signature de pourriel et de codes malveillants;

---

31 Industrie Canada, « L'économie numérique au Canada », http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00170f.html.

32 « L'hameçonnage est l'usurpation d'identité d'une personne ou d'un organisme de confiance dans le but de voler les renseignements personnels d'un individu, généralement dans un dessein de piratage d'identité. » *Ibid.*

33 Le lecteur est encouragé à dresser une courte liste de vendeurs en faisant sa propre recherche ou en retenant les services d'un expert en sécurité.

- bon nombre d'entreprises spécialisées en logiciels de protection offrent aujourd'hui des solutions axées sur les serveurs de courriel et les passerelles électroniques. Il devient de plus en plus important que ces deux points d'entrée au réseau de la cour soient protégés. Ces produits doivent être en mesure de détecter et de purger les fichiers infectés (tant les fichiers standard que les fichiers condensés) en temps réel;

- les applications du logiciel doivent pouvoir être gérées et surveillées depuis un pupitre de commande central;

- le logiciel doit comporter des applications permettant la gestion de politiques. Les fonctions importantes à cet égard comprennent celles de veiller à ce que les utilisateurs finals ne puissent contourner les lignes directrices relatives à la sécurité, d'utiliser la politique en matière de sécurité de la cour comme moyen d'éliminer ou de prévenir les intrusions par l'implantation de programmes malveillants, et de veiller à ce que l'agent de la sécurité informatique du système judiciaire soit avisé en cas d'atteinte à la sécurité.

Prévention

164. Les utilisateurs doivent être informés des risques de pourriel, de codes malveillants et de menaces connexes et recevoir une formation sur les meilleures méthodes de prévention. Cela est particulièrement important lorsque les utilisateurs ont accès à des renseignements judiciaires au moyen d'ordinateurs domestiques.

165. L'agent de la sécurité informatique du système judiciaire doit surveiller le processus d'approbation des nouvelles applications logicielles avant leur installation sur un ordinateur. Aucune application non autorisée ne peut être installée sur un ordinateur. Les juges doivent participer à l'établissement et à la révision d'une liste des applications autorisées. Sous réserve des Lignes de conduite sur la surveillance informatique (annexe 2), il y a lieu d'explorer les configurations logicielles tous les mois afin de s'assurer qu'aucun logiciel externe ou inconnu n'a été ajouté à un ordinateur.

166. Les logiciels devraient être téléchargés et installés uniquement par des administrateurs du réseau ou avec l'autorisation de ceux-ci (qui examineront ou feront l'essai de ces logiciels).

167. Les logiciels de protection devraient être installés sur les fichiers serveurs de façon à limiter la propagation des codes malveillants à l'intérieur du réseau. Les postes de travail devraient être munis d'un logiciel de protection installé en permanence et configuré de façon à balayer les données au fur et à mesure qu'elles entrent dans l'ordinateur. Tout le courrier électronique entrant devrait être balayé. Les programmes et fichiers ouverts au moyen d'applications vulnérables à des attaques de macro-virus ne devraient pas être exécutés sans un balayage préalable.

168. Il est vital que les fichiers de mise à jour des logiciels de protection du vendeur soient livrés automatiquement et installés par des moyens sûrs.

169. La formation du personnel en matière de sécurité devrait couvrir les renseignements suivants concernant les risques de codes malveillants et de pourriel :

- le logiciel de protection se limite à la détection des pourriels et des codes malveillants qui ont été identifiés précédemment. De nouvelles menaces plus sophistiquées font constamment leur apparition. Le logiciel de détection sera mis à jour continuellement au moyen de nouveaux fichiers de définition, de façon à pouvoir détecter les plus récentes menaces;

- tout le courriel et tous les fichiers provenant de l'extérieur de la cour doivent être balayés au fur et à mesure qu'ils sont reçus afin de vérifier s'ils comportent des codes malveillants, sous réserve des Lignes de conduite sur la surveillance informatique. Toute la vérification sera effectuée, s'il y a lieu, au niveau des pare-feux qui contrôlent l'accès aux réseaux, ce qui permettra une détection centralisée pour l'ensemble de l'organisation et réduira le temps inactif en assurant un balayage simultané des messages reçus qui sont adressés à plusieurs destinataires.

Détection et mise en œuvre des mesures de sécurité

170. Sous réserve des Lignes de conduite sur la surveillance informatique, le personnel chargé de l'administration du système devrait tenir et examiner tous les registres de détection et préparer les rapports connexes. Les utilisateurs doivent informer l'agent de la sécurité informatique du système judiciaire ainsi que les administrateurs du système de tout code malveillant qui est détecté ainsi que de tout changement apporté à la configuration ou comportement différent des systèmes ou applications informatiques.

171. Des mesures doivent être prises pour protéger la confidentialité de tous les courriels et fichiers entrants ou sortants de nature délicate qui sont saisis par un filtre de pourriel et transmis automatiquement à un administrateur.

172. Lorsqu'il est avisé qu'un code malveillant a été détecté, l'administrateur du système devrait informer l'agent de la sécurité informatique du système judiciaire et tous les utilisateurs ayant accès aux mêmes programmes ou données que leur système pourrait être compromis. Il y a lieu d'informer les utilisateurs des mesures qu'ils doivent prendre pour vérifier si leur système est compromis et pour éliminer la menace. Les utilisateurs devraient communiquer les résultats du balayage du système et de l'élimination de la menace à l'agent de la sécurité informatique du système judiciaire ainsi qu'aux administrateurs du système.

173. Tous les nouveaux logiciels doivent faire l’objet d’un test d’évaluation des performances et d’une vérification des codes malveillants avant d’être installés dans un ordinateur opérationnel.

174. Afin de pouvoir détecter les plus récents codes malveillants qui ont été identifiés, le logiciel de balayage devrait être mis à jour en temps réel au fur et à mesure que les mises à jour sont disponibles.

175. Tout ordinateur infecté par un code malveillant doit immédiatement être débranché du réseau. L’ordinateur ne devrait pas être raccordé au réseau avant que le personnel chargé de l’administration du système puisse s’assurer que la menace a été éliminée.

Annexe 1 : Recommandations du Comité consultatif sur la technologie, approuvées par le Conseil le 30 novembre 2001

1. Que le Conseil canadien de la magistrature tienne un séminaire à sa prochaine réunion semestrielle sur les questions urgentes de sécurité mises au jour dans le présent rapport (Sécurité technologique dans les cours : rapport du Comité consultative sur l'utilisation des nouvelles technologies par les juges).

2. Que le président du Conseil canadien de la magistrature transmette le présent rapport au Conseil canadien des juges en chef.

3. Que le président du Conseil canadien de la magistrature transmette le présent rapport aux sous-procureurs généraux et leur demande de collaborer à la mise en oeuvre des recommandations.

4. Que le Conseil canadien de la magistrature demande à l'Institut national de la magistrature et au Bureau du commissaire à la magistrature fédérale de coordonner la formation (sur les questions de sécurité du système d'information, y compris les préoccupations relatives à l'indépendance de la fonction judiciaire et à l'intégrité de l'information judiciaire) à l'intention des juges fédéraux et provinciaux ainsi que du personnel des technologies de l'information.

5. Que le Conseil canadien de la magistrature demande à tous les juges en chef de nomination fédérale ou provinciale :

   a) de faire la priorité à la sécurité du système d'information des cours;

   b) de veiller à l'élaboration immédiate d'une politique de sécurité, avant que la conversion à un système électronique ne survienne;

   c) d'identifier et d'obtenir les ressources financières requises, de personnel et autres ressources essentielles à la mise en oeuvre des mesures de sécurité appropriées;

   d) de faire en sorte qu'un membre du personnel en technologies de l'information relevant du juge en chef soit nommé à la gestion de la sécurité informatique des cours.

6. Pour des besoins d'uniformité, que le Conseil canadien de la magistrature assume un rôle de direction en autorisant le Comité consultatif sur la technologie d'élaborer un document provisoire englobant toutes les mesures de sécurité recommandées pour toutes les cours canadiens et fasse en sorte que le Comité dispose des ressources nécessaires à cette fin.

7. Plusieurs questions urgentes appellent une attention immédiate. Les points suivants doivent être considérés:

   a) Que le Conseil canadien de la magistrature demande au Comité consultatif sur la technologie d'élaborer un protocole de sécurité portant sur l'utilisation d'ordinateurs bloc-notes pendant leurs déplacements liés à leurs fonctions judiciaires.

   b) Que le Conseil canadien de la magistrature demande au Comité consultatif sur la technologie de collaborer avec les éditeurs spécialisés pour :

      i) établir une procédure visant à éviter la publication de jugements contenant des portions supprimées ou des modifications;

      ii) adopter un protocole assurant le retrait des jugements contenant des suppressions antérieures ou publiés accidentellement.

8. Que le Conseil canadien de la magistrature autorise le Comité consultatif sur la technologie de poursuivre les études pour faire des recommandations à l’égard d’une forme quelconque de surveillance extérieure de l’utilisation des ordinateurs par les juges et le personnel et lui assure les ressources nécessaires à cette fin.

Annexe 2 : Lignes de conduite sur la surveillance informatique

Recommandées par le Comité consultatif sur la technologie en juillet 2002 et approuvées par le Conseil canadien de la magistrature en septembre 2002.

(1) La surveillance informatique est, en général, exercée par l'intermédiaire d'un logiciel qui effectue un suivi des activités sur un ordinateur. Il est possible, entre autres, de faire le suivi des activités en réseau, des menaces à la sécurité, de l'utilisation de l'internet, de la saisie de données, de l'échange de courriels et des autres façons dont les ordinateurs sont utilisés. La surveillance est effectuée par une autre personne que l'utilisateur/e, soit à sa connaissance, soit à son insu. Dans un cas comme dans l'autre, l'utilisateur/e n'a aucun droit de regard sur la surveillance ou les données recueillies.

(2) Pour protéger efficacement les réseaux informatiques des menaces à la sécurité, une certaine surveillance est nécessaire. Dans certains cas, toutefois, la surveillance informatique peut menacer sérieusement l'indépendance de la magistrature et constituer par surcroît une atteinte illégale à la vie privée. Les présentes lignes de conduite visent à aider les juges et les administrateur/es de systèmes à élaborer des pratiques de surveillance informatique adéquates.

(3) Il est primordial de bien définir et d'être en mesure de justifier le but de la surveillance informatique des juges et du personnel judiciaire qui relève directement des juges. La surveillance informatique doit respecter le caractère secret des délibérations, la confidentialité, le droit à la protection de la vie privée et l'indépendance de la magistrature.

(4) Les informations que les juges et le personnel judiciaire conservent sur leur ordinateur ne peuvent dans aucune circonstance faire l'objet de surveillance informatique. Il est par conséquent défendu, entre autres, de surveiller tout ce qui est tapé à l'ordinateur, l'échange de courriels, les documents créés à l'aide de texteurs ou les autres fichiers informatiques, la recherche juridique, les sites internet visités et les fichiers téléchargés par chaque utilisateur.

(5) Des mesures peuvent être prises pour surveiller le trafic du réseau, tenir un journal des erreurs et des exceptions et effectuer une maintenance conforme aux normes de l'industrie pour préserver l'intégrité des ressources partagées en réseau et protéger les systèmes informatiques contre les cyberpirates et les menaces à la sécurité.

(6) La surveillance de la sécurité et de l'intégrité d'un système informatique :

n'est effectuée que pour des motifs légitimes, telles la vérification du rendement du réseau ou la gestion de la sécurité du réseau;

adopte l'approche la moins importune raisonnablement applicable dans les circonstances. Par exemple, si une activité en particulier a une incidence sur les ressources du réseau, les administrateur/es du système devraient tenter d'obtenir la collaboration des juges et du

personnel judiciaire leur faisant part de leurs préoccupations particulières en ce qui concerne les technologies de l'information;

ne recueille que des données d'ensemble. La surveillance des activités informatiques et des habitudes individuelles des juges ou du personnel judiciaire est prohibée, sauf s'il s'agit de vérifier si l'utilisateur/e a un droit d'accès valide.

(7) Les données relatives à la surveillance doivent être gardées confidentielles. Seul le personnel des technologies de l'information responsable de l'intégrité et de la sécurité du système informatique qui a besoin de ces données y a accès. Les journaux tenus sur la surveillance électronique et les autres fichiers doivent être régulièrement purgés. Il est permis de conserver des statistiques de surveillance mais seulement à partir de données d'ensemble et en se limitant aux éléments qui concernent l'intégrité et la sécurité du système.

(8) L'implantation de la surveillance informatique n'est jamais faite sans le consentement du juge en chef de la Cour. Les juges et le personnel judiciaire doivent participer activement à l'élaboration et à l'administration des pratiques en matière de surveillance informatique qui sont conformes aux présentes lignes de conduite. La surveillance informatique devrait être administrée par le personnel qui se rapporte directement au ou à la juge en chef de la Cour et qui relève directement de son autorité.

(9) Les juges et le personnel judiciaire doivent être tenus au courant des avis par des notifications claires, évidentes et régulières qui les informent sur les pratiques de surveillance. Les Cours devraient élaborer des lignes de conduite acceptables sur l'utilisation des ordinateurs et les communiquer aux intéressés lorsqu'on leur accorde un accès aux ordinateurs pour la première fois. Dès la mise en marche de l'ordinateur, l'écran devrait régulièrement afficher un rappel de l'existence et la raison des lignes de conduites sur la surveillance électronique et des raisons qui la justifient.

Annexe 3 : Protocole type pour les comités de technologie des tribunaux (2004)

Voir http://www.cjc-ccm.gc.ca/cmslib/general/Model_Protocol_FR.pdf

Annexe 4 : La protection en dix points des renseignements judiciaires informatisés

Guide établi à l'origine par le Sous-comité sur la sécurité informatique, Comité consultatif sur la technologie, Conseil canadien de la magistrature, le 15 mai 2002. Deuxième édition, 26 juillet 2006.

---

1. **Les appareils portatifs.** Gardez tous vos appareils portatifs (par exemple ordinateur portatif, téléphone mobile, Blackberry, assistant numérique personnel, support d'information amovible comme les unités de mémoire Flash USB) en votre possession lorsque vous voyagez. Autrement, verrouillez ces appareils au moyen d'un câble anti-vol et rangez-les dans le tiroir d'un bureau fermé à clé, dans le coffre-fort de l'hôtel ou dans le coffre de votre voiture.
2. **Les mots de passe.** Choisissez un mot de passe compliqué pour n'importe quel compte informatique. Utilisez au moins six caractères, quelque chose qui ne soit ni un nom propre ni un mot du dictionnaire. Utilisez également une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles, par exemple « FtLYd%7 ». Changez vos mots de passe régulièrement et ne les divulgez à personne. Pour conserver tous vos mots de passe, servez-vous d'un logiciel de gestion de mots de passe qui les protège tout en vous permettant de les récupérer facilement. N'écrivez jamais vos mots de passe à des endroits où d'autres personnes peuvent les voir.
3. **La sauvegarde.** Lorsque vous n'êtes pas connecté au réseau, veillez toujours à sauvegarder les fichiers importants. Vous pouvez utiliser une unité mémoire Flash USB, une unité de disque dur externe, une unité de bande magnétique, ou un CD ou DVD inscriptible. Assurez-vous que les fichiers sauvegardés soient chiffrés ou verrouillés, ou les deux.
4. **Le courriel.** N'ouvrez jamais des pièces jointes à un courriel d'une source inconnue et ne cliquez jamais sur un lien dans un courriel d'une source inconnue ou suspecte, surtout si l'auteur du courriel vous demande des renseignements personnels. De tels courriels pourraient être des tentatives d'« hameçonnage » ou de dangereux canulars se faisant passer pour de légitimes messages. Utilisez un filtre de pourriel pour réduire les risques d'intrusion.
5. **La protection contre les virus et les logiciels-espion.** Assurez-vous d'utiliser un logiciel anti-virus et anti-logiciel-espion. Les logiciels-espion, qui s'apparentent aux logiciels publicitaires, sont des exemples de codes malveillants qui prennent le contrôle des navigateurs Web, qui affichent des annonces publicitaires non sollicitées, et qui peuvent même épier vos activités informatiques. Assurez-vous de faire une mise à jour régulière du logiciel de protection et de configurer le logiciel de manière à vérifier automatiquement le courriel, les sites Web et les fichiers téléchargés.

6. **Les métadonnées.** Avant d'expédier des fichiers informatiques (comme des projets de jugement) à l'extérieur de l'environnement sécurisé de la cour, assurez-vous toujours de supprimer toutes les données cachées (les « métadonnées »), par exemple les révisions d'un texte, le texte supprimé de versions antérieures, ou des renseignements personnels. Voir l'article « Évitez le piège des métadonnées », paru dans le numéro d'octobre 2006 du bulletin *Actualités technologiques pour les juges*.
7. **Le chiffrement.** Utilisez une technologie de chiffrement fiable pour protéger les données particulièrement sensibles qui sont stockées dans votre ordinateur, que vous lez transmettiez ou non. Demandez au besoin l'aide de l'administrateur de système.
8. **La sécurité du système d'exploitation.** Lorsque vous recevez un message d'incitation de Microsoft Windows vous invitant à installer des pièces ou des correctifs sur votre système d'exploitation, confirmez la légitimité du message et installez ensuite la pièce ou le correctif pour vous assurer que votre système d'exploitation soit à jour. Les messages d'incitation de Microsoft ne sont jamais envoyés par courriel. Pour plus de renseignements à ce sujet, consultez le site Web de Microsoft sur la sécurité de l'informatique à l'adresse suivante : http://www.microsoft.com/canada/fr/athome/security/default.mspx.
9. **La sécurité de la réseautique sans fil.** Les réseaux sans fil sont d'une faiblesse notoire lorsqu'il s'agit de sécurité, mais une installation incorrecte peut vous exposer à des risques encore plus élevés. Assurez-vous de prendre toutes les mesures de sécurité possibles lorsque vous utilisez n'importe quel réseau sans fil. Utilisez l'équipement le plus récent de manière à bénéficier de la protection la plus actuelle en matière de sécurité de la réseautique sans fil.
10. **La surveillance.** La surveillance des ordinateurs des juges soulève de sérieuses questions concernant la vie privée, la confidentialité et l'indépendance des juges. Les juges en chef devraient s'adresser à l'administrateur de système compétent pour savoir dans quelle mesure et de quelle façon l'usage des ordinateurs par les juges et par le personnel judiciaire fait l'objet d'une surveillance.

Pour plus de renseignements, veuillez communiquer avec le Conseil canadien de la magistrature par courriel à info@cjc-ccm.gc.ca ou par téléphone au (613) 288-1566.

Annexe 5 : Glossaire de termes et d'acronymes définis[34]

Terme ou acronyme	Sens
AC	Autorité de certification - organisme fiable qui attribue des certificats numériques aux personnes afin d'authentifier leur identité
Authentification	Processus qui consiste à vérifier l'identité déclarée d'une personne
Bluetooth	Technologie sans fil qui permet à des appareils électroniques d'échanger entre eux de la voix et des données sur une courte distance.
Certificat	Document numérique qui sert à authentifier l'identité de l'expéditeur
Cheval de Troie	Programme apparemment inoffensif qui contient un logiciel malveillant
Chiffrement	Transformation d'un texte lisible par l'utilisateur en code illisible afin de protéger l'information de l'accès non autorisé
Cryptogramme	Texte chiffré
Cryptographie	La science du chiffrement
CST	Centre de la sécurité des télécommunications
EMR	Évaluation des menaces et des risques
FAI	Fournisseur d'accès Internet - organisme qui fournit l'accès à l'Internet
Hameçonnage	Usurpation d'identité d'une personne ou d'un organisme de confiance dans le but de voler les renseignements personnels d'un individu, généralement dans un dessein de piratage d'identité
ICP	Infrastructure à clé publique - système de certificats et d'autorisations numériques qui vérifie l'autorisation de chaque personne participant à une transaction électronique
IDS	Système de détection d'intrusion - système qui surveille les tentatives en vue d'obtenir l'accès à un réseau

[34] Le Webopedia est un excellent dictionnaire en ligne gratuit dans le domaine de l'informatique et de la technologie d'Internet. Il peut être consulté en ligne à http://www.webopedia.com .

Terme ou acronyme	Sens
Intrusion	L'intrusion est définie comme une tentative visant à compromettre la sécurité d'un ordinateur ou d'un réseau. La détection d'intrusion est le processus qui consiste à surveiller les évènements qui surviennet dans le système informatique ou dans le réseau et à les analyser pour détecter des signes d'intrusions.
JCIT	Judicial Committee on Information Technology (Texas) (Comité judiciaire sur les technologies de l'information)
JUDICOM	JUDICOM est l'acronyme de communication judiciaire. Il s'agit d'un outil collaboratif électronique développé par le Bureau du Commissaire à la magistrature fédérale afin de brancher à l'autoroute de l'information les juges nommés par le fédéral au Canada.
Logiciel-espion	Code malveillant qui recueille secrètement des renseignements sur un utilisateur par la voie d'Internet et qui est souvent téléchargé sans le savoir en même temps qu'un logiciel gratuit ou partagé.
Pourriel	Courrier électronique non sollicité et envoyé massivement.
Pare-feu	Un produit matériel ou un logiciel programmé pour filtrer les intrusions non désirées d'un ordinateur ou d'un réseau à un autre
Personnel judiciaire	Tout employé ou contracteur qui rend compte directement aux juges et dont le travail inclut de manipuler des renseignements judiciaires.
RAS	Serveur d'accès à distance
Renseignements judiciaires	Tous les renseignements, quel qu'en soit la forme ou le format, qui sont créés ou utilisés au soutien de fonctions judiciaires
RL	Réseau local - système qui relie des utilisateurs à des ressources informatiques partagées à l'intérieur d'un immeuble
RL sans fil	Réseau local qui fonctionne par radiofréquence au lieu d'être branché au moyen de câbles
Sauvegarde	Procédure qui consiste à copier régulièrement les renseignements critiques concernant le système et la configuration ainsi que les documents afin d'en assurer la disponibilité en cas de perte des données se trouvant sur les serveurs et les postes de travail.
Sécurité matérielle	La sécurité matérielle s'entend de la protection des immeubles et de l'équipement (ainsi que des renseignements et logiciels qui s'y trouvent) des introductions par effraction, vols, actes de vandalisme, catastrophes naturelles et autres et dommages accidentels.

Terme ou acronyme	Sens
Sécurité informatique	Sécurité des technologies de l'information
SRA	Accès à distance protégé - protection offerte aux utilisateurs branchés à un réseau local depuis une installation extérieure
SSID	Identificateur de service - employé dans les réseaux locaux sans fil
SSL	Couche de sockets sécurisés - protocole de chiffrement permettant l'envoi de données en privé sur le Net
Temps réel	Dans le cas des programmes de protection antivirus, système de distribution dans le cadre duquel les mises à jour desdits programmes sont disponibles au fur et à mesure qu'elles sont créées et non seulement en fonction d'un calendrier prédéterminé, ce qui pourrait retarder la mise en oeuvre
Texte en clair	Texte que peut lire l'utilisateur avant le chiffrement et après le déchiffrement
TI	Technologie de l'information
UPS	Alimentation sans coupure - bloc-batterie spécial pouvant alimenter un serveur ou un ordinateur pendant un court laps de temps sans qu'il y ait perte de données en cas de panne du système de courant principal
Utilisateurs judiciaires	Les juges et le personnel judiciaire
Ver	Type spécial de virus qui se reproduit
Virus	Programme malveillant qui se propage d'un utilisateur à l'autre sur un réseau
VPN	Réseau privé virtuel – logiciel qui permet aux utilisateurs de communiquer en privé en utilisant les réseaux publics

Annexe 6 : Modèle de règles d'utilisation acceptable des ordinateurs pour le personnel judiciaire

Approuvé par le Comité exécutif du Conseil canadien de la magistrature le 5 décembre 2003

1.0 Aperçu général

1. Le gouvernement <fédéral/provincial> met des moyens informatiques à la disposition des juges et du personnel de soutien judiciaire dans l'exercice de leurs fonctions.

2. Les présentes règles énoncent, en ce qui concerne l'utilisation des moyens informatiques, des lignes directrices qui serviront à protéger ces moyens contre les actions illicites ou dommageables, qu'elles soient délibérées ou non, à assurer le rendement optimum des systèmes d'ordinateur pour tous les juges et le personnel de soutien judiciaire, et à permettre aux juges et au personnel de soutien judiciaire de faire un certain usage de ces moyens à des fins personnelles, contribuant à renforcer leur efficacité et productivité.

3. Le premier objectif est de protéger l'appareil judiciaire et la sécurité des données judiciaires par le maintien d'une protection efficace, ce qui requiert la participation et la coopération de chacun des juges et des membres du personnel de soutien qui fait usage des données et/ou des systèmes d'information. Un abus des moyens informatiques expose l'appareil judiciaire à certains risques, tels les attaques virales, la compromission des systèmes et services du réseau, les problèmes légaux, les atteintes éventuelles à la sécurité et la diminution de l'efficacité du réseau.

2.0 Objet

Les présentes règles ont pour objet de définir l'usage acceptable et les pratiques exemplaires concernant les moyens informatiques au sein de la <désignation de la juridiction concernée>.

3.0 Champ d'application

Les présentes règles s'appliquent aux juges et au personnel de soutien judiciaire. Le juge en chef peut les étendre aux fournisseurs, aux consultants, aux employés judiciaires temporaires et autres, en les incorporant par référence dans les contrats ou mémoires d'entente à titre de condition pour l'utilisation des moyens informatiques.

4.0 Définitions

Aux fins des présentes règles les définitions qui suivent s'appliquent

Moyens informatiques s'entend notamment des ordinateurs portatifs, des ordinateurs personnels et de leurs périphériques, du logiciel, de la connectivité Internet, de l'accès aux services Internet/Intranet/Extranet/VPN, et du courriel. Cette liste donne juste quelques exemples de moyens informatiques soumis aux présentes règles; elle n'est pas exhaustive.

Temps libre de l'employé s'entend des périodes où le personnel de soutien judiciaire n'est pas censé exercer ses fonctions, comme par exemple les heures hors service qui précèdent ou suivent une journée de travail, les pauses-déjeuner ou autres pauses autorisées.

Personnel de soutien judiciaire s'entend des employés qui sont directement sous les ordres des juges : adjoints judiciaires, secrétaires, consultants, étudiants stagiaires et clercs.

Usage personnel restreint s'entend de l'utilisation des moyens informatiques par les juges et le personnel de soutien judiciaire en dehors de l'exercice de leurs fonctions, par exemple pour les activités professionnelles, le perfectionnement, et l'usage personnel accessoire dans les limites du raisonnable. Est exclue la modification des moyens informatiques en usage, par exemple la modification de la configuration.

Surcroît de dépenses minimal s'entend du fait que l'usage des moyens informatiques ne doit avoir pour autre résultat que l'usure normale ou la consommation de très peu d'électricité, d'encre, de poudre imprimante ou de papier. À titre d'exemple, il s'agit de se servir de l'imprimante de l'ordinateur pour imprimer un nombre limité de pages, d'envoyer rarement des courriels et d'utiliser l'Internet occasionnellement.

5.0 Règles

5.1 Sécurité et renseignements exclusifs

1. Les juges et le personnel de soutien judiciaire qui utilisent des moyens informatiques fournis par le gouvernement <fédéral/provincial> ont la responsabilité de se familiariser avec les présentes lignes directrices et de les respecter dans l'exercice de leurs activités.

2. Les juges et le personnel de soutien judiciaire doivent prendre toutes les mesures nécessaires pour prévenir l'accès non autorisé aux renseignements confidentiels.

3. Les juges et le personnel de soutien judiciaire doivent chiffrer les renseignements à protéger, conformément aux lignes directrices de la Cour en matière de sécurité. Les projets de jugement doivent être chiffrés avant d'être envoyés par courriel au personnel de soutien judiciaire ou à d'autres juges, à moins que la transmission ne se fasse dans JUDICOM ou un système de courriel interne sûr.

4. Le service <fédéral/provincial> de Technologie de l'information peut, avec le consentement du juge en chef, exercer une surveillance limitée sur les moyens et les systèmes informatiques ainsi que sur le trafic sur le réseau informatique, conformément aux lignes directrices en matière de contrôle approuvées par le Conseil canadien de la magistrature, et conformément aux présentes lignes directrices. Dans le but d'assurer l'intégrité des ressources partagées du réseau et de protéger les systèmes informatiques contre les menaces à leur sécurité, des procédures peuvent être mises en œuvre pour surveiller le trafic sur le réseau, consigner les erreurs et les exceptions, et assurer la maintenance des moyens informatiques conformément aux normes de l'industrie. Par contre, aucune surveillance fondée sur le contenu des données n'est autorisé.

5. Les juges et le personnel de soutien judiciaire sont responsables de la sécurité de leur mot de passe et de leur compte. Les mots de passe doivent être protégés, et les comptes ne doivent pas être partagés. Les mots de passe doivent être changés tous les trimestres au niveau du système, et tous les six mois au niveau individuel. Il ne faut pas utiliser le même mot de passe pour différents comptes, et il ne faut pas le consigner dans l'ordinateur ou le navigateur Web. Le mot de passe doit comprendre au moins six caractères en une combinaison de chiffres, de lettres et de caractères alphanumériques; il ne faut pas que ce soit un mot ayant une signification.

6. Tous les ordinateurs, ordinateurs portatifs et postes de travail doivent être sécurisés au moyen d'un économiseur d'écran protégé par mot de passe avec activation automatique toutes les 10 minutes ou moins, ou par la fermeture de la session si l'ordinateur est laissé sans surveillance.

7. Les données mémorisées dans les ordinateurs portatifs étant particulièrement vulnérables, il ne faut jamais laisser ces derniers sans surveillance mais, si possible, les protéger par un mot de passe d'accès ou par un câble anti-vol.

8. Les juges et le personnel de soutien judiciaire doivent mettre fin à leur système et éteindre leur ordinateur à la fin de la journée de travail.

9. Tous les ordinateurs utilisés par les juges et le personnel de soutien judiciaire et branchés sur le réseau Internet/Intranet/Extranet/VPN de la Cour, qu'ils leur appartiennent en propre ou soient la propriété du <gouvernement fédéral/provincial>, doivent exécuter continuellement un programme approuvé et à jour de détection des virus.

10. Les juges et le personnel de soutien judiciaire doivent être prudents lorsqu'il s'agit d'ouvrir les pièces jointes au courriel envoyé par des inconnus, car elles peuvent contenir des virus.

11. Les documents importants et les travaux produits doivent être sauvegardés pour mémoire dans un serveur ou autre support sécurisé et fiable, conformément aux modalités de sauvegarde fixées par la Cour.

12. Il faut observer les procédures appropriées pour s'assurer que les jugements et autres documents transmis à l'extérieur de l'environnement sécurisé de la Cour ne renferment ni information cachée ni méta données, tels les révisions ou ratures sur des projets antérieurs ou des renseignements confidentiels.

13. Lorsqu'il s'agit de se débarrasser des ordinateurs, lecteurs, disquettes ou autres supports de mémoire, il faut observer des procédures qui soient adaptées à la sensibilité des données mémorisées. Il ne suffit pas d'effacer les fichiers, il faut les formatter avant de recycler ou de réutiliser les supports de mémoire. Dans certains cas, il faut détruire ces supports, conformément aux politiques en la matière de la Cour.

5.2 Usage personnel restreint

1. Les moyens informatiques servant dans l'exercice des fonctions judiciaires peuvent être utilisés à des fins personnelles à condition que cet usage ne coûte rien ou très peu aux contribuables. Pareil usage peut ajouter à l'efficacité et à la productivité des juges et du personnel de soutien judiciaire dans leur vie professionnelle et personnelle. Il peut aussi être utile aux juges qui doivent se déplacer pour présider des audiences à l'extérieur de leur ville de résidence.

2. Un usage personnel restreint des moyens informatiques est permis aux membres du personnel de soutien judiciaire s'il n'entrave pas l'exercice de leurs fonctions et n'occasionne qu'un surcroît de dépenses minime. Il ne peut avoir lieu que pendant leur temps libre, et peut être supprimé ou réduit à n'importe quel moment par le juge en chef.

3. Un usage personnel restreint des moyens informatiques est permis aux juges s'il n'entrave pas l'exercice de leurs fonctions et n'occasionne qu'un surcroît de dépenses minime.

4. Lorsqu'ils utilisent à titre personnel et de façon restreinte les moyens informatiques mis à leur disposition, les juges et le personnel de soutien judiciaire doivent toujours se garder de donner l'impression qu'ils le font à titre officiel. Si cet usage personnel restreint est susceptible d'en donner l'impression, il faut ajouter un désaveu, par exemple : « Le contenu de ce message est personnel et ne représente pas les vues des juges ou de la Cour. »

5. Les contributions que les juges ou le personnel de soutien judiciaire envoient à partir d'une adresse électronique de la Cour à un forum privé doivent comprendre l'avertissement que les opinions exprimées sont strictement celles de l'auteur et non pas nécessairement celles de la Cour, à moins que cette contribution ne soit faite dans le cadre de ses fonctions officielles.

   Les usagers doivent s'abstenir d'utiliser les adresses électroniques de la Cour relativement à leurs contributions personnelles à un forum public ou aux messages personnels qu'ils affichent sur un babillard public. La raison d'être de cette règle est que de telles contributions ou de tels messages accroissent les risques de ciblage à des fins de marketing ou à des fins malveillantes.

5.3. Usage inacceptable

L'usage inacceptable des moyens informatiques s'entend de ce qui suit :

5.3.1. Manœuvres visant à déjouer la protection

a) contourner l'authentification de l'usager ou la protection d'un ordinateur, réseau ou compte, quel qu'il soit.

b) entraver ou empêcher le service pour tout autre usager.

c) utiliser un programme/script/commande, quel qu'il soit, ou envoyer des messages, quels qu'ils soient, pour entraver ou désactiver une session de tout autre usager, par quelque moyen que ce soit, localement ou par Internet/Intranet/Extranet/VPN.

5.3.2. Atteinte au rendement

a) tout usage personnel qui pourrait causer l'encombrement, le retard ou l'interruption du service pour le système de quelque juridiction ou gouvernement que ce soit, par exemple le téléchargement de gros fichiers audio ou vidéo.

b) l'utilisation des moyens informatiques de façon à causer une perte de productivité, à entraver l'exercice des fonctions officielles, ou à causer un surcroît de dépenses appréciable pour le Trésor public.

5.3.3. Actes illicites ou immoraux

a) l'utilisation des moyens informatiques à des fins illicites, ce qui s'entend des infractions criminelles, des contraventions aux lois et règlements non pénaux, fédéraux et provinciaux, et de toute action qui expose un individu ou une institution à une action civile.

b) la transmission non autorisée de données judiciaires aux forums, babillards ou autres sites publics, y compris toute utilisation qui pourrait donner l'impression que la communication a été faite à titre officiel.

c) la création ou l'envoi de lettres en chaîne, de courriel spam ou autres messages à diffusion massive, quel qu'en soit le sujet, sans y être autorisé ou sans que les destinataires en aient fait la demande.

d) l'utilisation des moyens informatiques à des fins professionnelles ou commerciales privées.

e) Les activités suivantes sont aussi interdites, sauf dans la mesure où elles sont requises dans l'exercice des fonctions judiciaires :

   i) la création, le téléchargement, la visualisation, la sauvegarde, ou la transmission de représentations explicites d'actes sexuels, de documents inappropriés ou offensants pour les collègues ou pour le public, par exemple la propagande haineuse, ou de documents touchant aux jeux de hasard illégaux et à d'autres activités illégales ou interdites.

ii) la communication, à des gens de l'extérieur qui ne font partie ni de la Cour ni du ministère de la Justice, de données confidentielles de la Cour ou de données judiciaires confidentielles, notamment des listes de juges ou de membres du personnel de soutien judiciaire.

5.3.4. Atteinte à la protection du système

a) l'introduction dans les réseaux ou serveurs des programmes destructeurs, tels les virus.

b) la révélation du mot de passe d'un compte à autrui, à moins que ce ne soit à un usager autorisé et conformément à la politique de la Cour.

c) le fait de permettre à d'autres, y compris aux membres de la famille et du ménage, de se servir du mot de passe d'un compte ou de se servir d'un ordinateur connecté au VPN ou à l'Extranet de la Cour, en cas de travail fait à la maison.

d) le fait d'essayer d'accéder sans autorisation à d'autres systèmes.

5.3.5. Infractions techniques

a) créer des brèches de sécurité ou perturber les communications dans le réseau. Brèche de sécurité s'entend entre autres de l'accès aux données qui ne sont pas destinées au juge ou au membre du personnel de soutien judiciaire concerné, accéder à un serveur ou un compte auquel il ne possède pas les permissions d'accès, à moins que ces activités soient requises dans le cadre normal de ses fonctions.

b) exploration du point d'accès ou du dispositif de protection, sauf autorisation préalable du service de Technologie de l'information.

c) toute manoeuvre de surveillance du réseau qui intercepte des données qui ne sont pas destinées au juge ou à l'employé concerné.